



Level 4, 21 Terminal Avenue
Plaza Offices - West
Canberra Airport ACT 2609
Phone: 02 6275 2222
www.canberraairport.com.au

12 February 2025

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600
By email: pjcis@aph.gov.au

Dear Committee Secretary

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

Canberra Airport appreciates the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security concerning the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024.

Canberra Airport hopes the enclosed submission assists the Committee in its review of the Bill.

For more information, please contact our Government Relations and Policy Advisor,

Yours sincerely

Michael Thomson
Head of Aviation



FEBRUARY 2025

TRANSPORT SECURITY AMENDMENT (SECURITY OF AUSTRALIA'S TRANSPORT SECTOR) BILL 2024

Submission to the Parliamentary Joint Committee on
Intelligence and Security



TABLE OF CONTENTS

Introduction	3
Unlawful interference	3
Cyber security incidents	3
Reporting timeframes	4
Security assessments	4
All hazards security framework	4
Annual statements of compliance	5
Powers of security inspectors	5
Vulnerability testing	5
Security directions	5
Expanding special security directions	5
Test weapons	6
Amending the definition of a test weapon	6
Cost of regulation	6
Conclusion	7

INTRODUCTION

Canberra Airport appreciates the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security in relation to the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024. This submission relates specifically to the proposed amendments to the *Aviation Transport Security Act (ATSA) 2004*.

This Committee's review complements the consultation by the Department of Home Affairs in mid-2024 on reforming the ATSA. At the time, Canberra Airport provided a detailed submission to the Department seeking to clarify some proposals that were presented in a generalised manner and appeared difficult to apply to actual incidents. Following this, the Department committed to further consultation to improve the overall effectiveness and applicability of the reforms without adversely impacting aviation industry participants. It is hoped the Committee's review of the Bill will supplement this undertaking by the Department.

The Australian aviation sector is critical for the movement of people and goods. In recent years, however, a pandemic, natural disasters and malicious actors have impacted the sector causing significant ramifications for passengers, airports and airlines. This has threatened the industry's ability to deliver services to passengers and businesses, while risking the security of critical infrastructure. By working together, aviation industry participants and the government can reduce further threats to the security and resilience of the sector. The amendments proposed will hopefully achieve this.

By considering potential improvements to the Bill, the Committee can ensure the amendments to the ATSA achieve the objectives set out by the Department, while balancing the needs of aviation industry participants. Canberra Airport provides the following commentary on the Bill to support the work of the Committee.

UNLAWFUL INTERFERENCE

Cyber security incidents

Canberra Airport recognises the risk posed to the aviation sector of increasing cyber security incidents. The Bill would expand the definition of an "unlawful interference with aviation" to include cyber security incidents, ensuring the transport sector is in line with every other sector of critical infrastructure.¹ It is hoped this will support airports to implement measures to effectively respond to cyber security incidents while limiting the impact on operational capabilities.

Canberra Airport supports the proposal to expand reporting requirements to the Australian Signals Directorate (ASD) if a cyber security incident causes a "reasonable impact" or "significant impact", rather than law enforcement agencies (as is the case for other security incidents).² The ASD is equipped with the resources and expertise to support aviation industry participants to appropriately respond to a cyber security incident. However, it is critical that additional administrative and regulatory burden is not

¹ *Explanatory Memorandum, Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (Cth)*.

² *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (Cth)*.

placed on industry participants while in the midst of a potential cyber security incident. This requirement to liaise directly with ASD is in addition to mandatory reporting to the Department.

Reporting timeframes

There must be more consistency between the proposed reporting timeframes for cyber security incidents and existing security incidents defined as "unlawful interference with aviation".³ The amendments to the ATSA state that airport operators (Section 100) and employees of aviation industry participants (Section 103) must report cyber security incidents that cause a "significant impact" within 12 hours to the relevant authorities.⁴ Those incidents considered to cause a "reasonable impact" must be reported within 72 hours.⁵ However, existing reporting timeframes for other security incidents – including persons taking unauthorised control of an aircraft or an act being committed that place the safe operation of an airport at risk – must be "reported as soon as possible, but no later than 24 hours after the security incident is identified".⁶

The inconsistent reporting standards have the potential to cause confusion for aviation industry participants who may inadvertently not meet their reporting obligations. Given failure to comply with this requirement will be a strict liability offence, either the airport operator or an employee of an aviation industry participant may be penalised simply due to an administrative misunderstanding. Consideration of adopting a standard reporting timeframe for all acts of "unlawful interference with aviation" of no later than 24 hours after the incident is identified would reduce the likelihood of this occurring.

SECURITY ASSESSMENTS

All hazards security framework

Canberra Airport appreciates the need for greater consideration of hazards that interfere with the operations of the aviation sector beyond unlawful acts. The COVID-19 pandemic and the 2019-20 Black Summer bushfires greatly impacted the ability of aircraft to arrive and depart from Canberra Airport. The cascading consequences of these hazards significantly affected passengers, the airport and airlines.

Through existing mandatory reporting obligations with ACT and Commonwealth Government agencies, Canberra Airport has been able to mitigate and respond to operational interferences across the spectrum of risks identified by the Department. Duplicating administrative obligations for aviation industry participants will be labour intensive and may require a reallocation of staffing to comply.

³ *Aviation Transport Security Act 2004* (Cth).

⁴ *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024* (Cth).

⁵ *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024* (Cth).

⁶ *Aviation Transport Security (Incident Reporting) Instrument 2018* (Cth).

Annual statements of compliance

The requirement for aviation industry participants to provide annual statements of compliance regarding their transport security programs (TSP) may create additional administrative and financial burdens. A review of Canberra Airport's TSP commenced in the first quarter of 2024 with ongoing engagement between the airport and the Department to ensure each security measure complied with legislative requirements. This has been a lengthy process. As of the second week of February 2025, approval for the updated TSP has still not been received from the Department.

Administrative and regulatory procedures related to the security of critical infrastructure should not be expedited for the benefit of regulators or industry participants. However, the significant amount of time that has been dedicated by both Canberra Airport and the Department to the TSP review process over the past 12 months demonstrates how labour and resource intensive it can be. Given reviews take place every two years, the annual statement of compliance will result in aviation industry participants being in a continual cycle of regulatory reporting.

Introducing annual compliance reporting requirements for TSPs, which are already closely monitored by airport employees and Department officers may also create administrative backlogs that causes approval delays. There must not be a repeat of the delays that occurred once the issuing of Aviation Security Identification Cards (ASIC) transitioned to AusCheck in 2023, resulting in some operational airport staff waiting more than four months for their renewal applications to be approved.

POWERS OF SECURITY INSPECTORS

Vulnerability testing

Canberra Airport supports the use of vulnerability testing to identify potential flaws in technology, processes and personnel, particularly with the increasing risk of emerging threats. However, it should not become a mandatory component of compliance testing.

It would be appropriate for vulnerability testing to occur on a provisional basis to assist aviation industry participants strengthen security systems, rather than be used as an additional compliance tool. Canberra Airport supports greater investment in education on emerging risks and threats rather than increased compliance. This will be a more effective strategy to improve Australia's aviation security landscape.

SECURITY DIRECTIONS

Expanding special security directions

The expansion of special security direction (SSD) powers in response to emerging threats and risk will likely be an effective tool. Throughout the consultation process conducted by the Department, there was limited focus on the financial, operational and administrative impacts for aviation industry participants

before an SSD is issued. This has also not been examined in the Bill or the Explanatory Memorandum. Further information on these potential impacts would be welcomed by aviation industry participants.

It is noted that SSDs will only be used as a last resort, however, the wording of the amendment in the Bill is quite broad: "a general threat of unlawful interference with aviation is made or exists".⁷ It is important that despite this, SSDs will not be overused and enacted without proper consideration. If this were to occur, it would likely expose aviation industry participants to additional regulatory and administrative burden that would have a detrimental impact on operational capability.

TEST WEAPONS

Amending the definition of a test weapon

The decision to update the definition of a test weapon will provide aviation security inspectors with an improved assortment of instruments to conduct compliance checks of screening points at airports. This will ensure screening officers are exposed to existing and emerging threats and will therefore be an effective means of improving education and knowledge acquisition. Canberra Airport supports enhancing the skills of screening officers across the aviation sector and this will likely be achieved through this initiative.

COST OF REGULATION

As outlined in the impact analysis prepared by the Department, the initial and ongoing costs of these amendments will be significant for aviation industry participants. At a minimum, the aviation and maritime sectors will be expected to pay \$190 million just to implement the proposals, yet this could grow to \$336 million.⁸ Ongoing annual costs are forecast to be between \$115 million and \$203 million.⁹ These are in addition to costs associated with existing security measures.

It should be noted that costs incurred by airports to establish and maintain security measures are generally recovered from airlines, who subsequently pass these on to passengers through airfares. As such, the Committee is encouraged to consider the additional cost of regulation that will be borne by the travelling public. Due to economic pressures, many households are unable to justify travelling because of high airfares. Industry and government must collaborate on reducing airfares to increase visitation and visitor spend, particularly throughout regional Australia. It is, therefore, important that a consequence of strengthening the security of the aviation industry is not increased airfares.

⁷ *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024* (Cth).

⁸ Department of Home Affairs, *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024: Impact Analysis for Final (Second Pass) Assessment*, 2024, 47.

⁹ Department of Home Affairs, *Impact Analysis for Final (Second Pass) Assessment*, 47.

CONCLUSION

Canberra Airport supports measures that safeguard against unlawful interference with critical infrastructure such as airports. The proposed amendments in this Bill will strengthen the resilience and security of aviation industry participants. As discussed in this submission, there must be consideration of the additional administrative and regulatory burden these measures will create for industry participants, with many already complying with mandated requirements under other legislative instruments.

Canberra Airport appreciates the opportunity to provide a submission. It is hoped the perspective offered will assist the Committee in its review of the Bill.



