Australian Government

Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report:

Advisory report on the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024

OCTOBER 2025

The Government thanks the Parliamentary Joint Committee on Intelligence and Security (‘Committee’) for its review of the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (‘the Bill’).

The Government notes that the *Transport Security Amendment (Security of Australia's Transport Sector) Act* became law on 28 March 2025.

The Government provides the following responses to the Committee’s recommendations.

Recommendations

Recommendation 1.1: The Committee recommends that any new or amended regulations arising from changes to the *Aviation Transport Security 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) provide greater clarity and guidance to industry on key elements of the reforms, including definitions, liabilities, and interaction with other relevant legislation.

Response:

Agree in-principle. The Department of Home Affairs (the department) will ensure that any new or amended regulations will provide greater clarity and guidance to industry on key elements of the reforms.

Recommendation 1.2: The Committee recommends that the Department of Home Affairs work with industry to develop the regulations and instruments as part of a genuine consultative process.

Response:

Agree. The department will continue to consult with industry to develop the regulations and instruments.

Recommendation 2.1: The Committee recommends that the Department of Home Affairs, as the regulator, offer clear and accessible guidance and training to aviation and maritime industry participants on the new security obligations and incident reporting requirements, with a particular focus on supporting smaller entities to meet their compliance obligations.

Response:

Agree in-principle. The department will consult with industry to develop the new security obligations and incident reporting requirements, and provide industry with clear and accessible guidance on what those obligations and requirements are, with a focus on supporting smaller entities to meet their compliance obligations.

Recommendation 2.2: The Committee further recommends that the Australian Government ensure that the Department of Home Affairs continues to be adequately resourced to fulfil all its responsibilities as the regulator.

Response:

Noted. Recent security incidents at airports and seaports highlight the need to ensure that, as the regulator, the department can undertake the full range of compliance activities to ensure the security of Australia's aviation and maritime sectors.

Recommendation 3: The Committee recommends that the Department of Home Affairs work with Commonwealth partners to:

- **identify and address any duplication of reporting requirements, particularly in relation to cyber security incident reporting**
- **prioritise the development of a single Commonwealth reporting portal for the reporting of cyber security incidents**
- **pending the full implementation of such a portal, take whatever collective measures are necessary to facilitate coordinated and efficient reporting that meets the needs of the Australian Government while minimising duplication and the burden on industry.**

Response:

Agree in-principle. The department will work with Commonwealth partners to identify and address any duplication of reporting requirements, particularly in relation to cyber security incident reporting.

The department is working across Government to streamline cyber security incident reporting and reduce duplicative reporting requirements for regulated entities, as part of Horizon 1 of the 2023-2030 Australian Cyber Security Strategy. Currently, the department is working with stakeholders to explore non-legislative, low or no cost technological enhancements to the current single reporting portal on cyber.gov.au.

Pending the full implementation of the single reporting portal, where possible, the department will take measures necessary to facilitate coordinated and efficient reporting that meets the needs of the Australian Government while minimising duplication and the burden on industry. This includes ensuring that the cyber incident reporting obligation under these reforms is consistent with existing reporting obligations on the ReportCyber portal at cyber.gov.au, to minimise regulatory burden.

Recommendation 4: The Committee recommends that the Australian Government consider amendments to the Bill that would allow for a penalty regime that is responsive and scalable, whilst also noting the desirability of consistent penalties across critical industries.

Response:

Agree in-principle. The Government considered, and made, amendments to the Bill that will allow for a penalty regime that is responsive and scalable.

Recommendation 5: The Committee recommends that the Bill be amended so that the use of the expanded security directions powers in the ATSA and the MTOFSA will:

- **only be used as a last resort, when there are no other effective measures to prevent or mitigate the impacts of an threat of unlawful interference**
- **require the Secretary to take certain things into account before deciding to exercise the powers**
- **be subject to additional safeguards and accountability for the Secretary, including Ministerial authorisation or notification requirements.**

Response:

Agree in-principle. The Government considered, and made, amendments to the Bill regarding the use of security directions powers.

Recommendation 6: The Committee recommends that the Government consider providing extended implementation timeframes for smaller affected entities, such as regional airports, for example.

Response:

Agree in-principle. The department will consider providing extended implementation timeframes for smaller affected entities. The all hazards security obligations will be subject to industry consultation as part of regulatory amendments and be scaled relative to an entity's operating environment and size to ensure regulation remains proportionate.