

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

Impact Analysis for Final (Second Pass) Assessment

Prepared by the Department of Home Affairs



# Australian Government

This Impact Analysis (IA) analyses the outcomes of consultation conducted by the Department of Home Affairs with industry on the regulation of Australia’s aviation and maritime sector industry participants. This document aims to provide transparency on the government’s decision-making process and has enabled the testing of regulatory impacts of options under consideration with stakeholders.

# Contents

Executive Summary

Introduction

1. What is the policy problem you are trying to solve and what data is available?
2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured
3. What policy options are you considering?
4. What is the likely net benefit of each option?
5. Who did you consult and how did you incorporate their feedback?
6. What is the best option from those you have considered and how will it be implemented?
7. How will you evaluate your chosen option against the success metrics?

# Executive Summary

Australia's transport sector, is essential for the nation's social and economic prosperity, national security, and defence, and for facilitating the provision of essential goods and services.

The 2023 Critical Infrastructure Resilience Strategy defines critical infrastructure as:

"...physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security." <sup>1</sup>

The evolving, dynamic and heightened geopolitical and cyber threat environment facing Australia requires regular review of current legal parameters to ensure the integrity and resilience of critical infrastructure.

The Department of Home Affairs (the department) remains focused on ensuring the security and resilience of Australia's critical infrastructure, including for Australia's transport sector (comprising aviation, maritime and offshore facility industry participants). This involves providing ongoing assurance that the Australian government is managing critical infrastructure in a manner which reflects an inherently complex risk environment.

Australia's transport sector is security-regulated through the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) and supporting regulations (transport security legislative frameworks). The transport security legislative frameworks require the transport sector to mitigate the threat of unlawful interference, terrorism, and serious crime within an entity's physical boundary or geographical location. However, the limited focus of the transport security legislative frameworks does not reflect the current or emerging threat environment nor the range of risks the Australia's transport sector faces.

The department's role in assuring the security of the transport sector involves ongoing assessment of whether the applicable legislation remains fit for purpose. It also requires engagement with industry to understand and address areas of concern. As such, the department is proposing to amend the existing transport security legislative frameworks to ensure that it:

- **operates on a flexible, risk-based and scalable basis**, ensuring obligations are adaptable and flexibly applied to an appropriate range of entities and their specific risk environments
- **holistically addresses potential vulnerabilities** which could have a relevant impact on aviation and maritime entities and flow-on effects for Australia's critical infrastructure, which will result in security requirements that support the delivery of dynamic and modernised transport security legislative frameworks

---

<sup>1</sup> Critical Infrastructure Resilience Strategy, CISC, 2023, [cisc.gov.au/critical-infrastructure-resilience-strategy](https://www.cisc.gov.au/critical-infrastructure-resilience-strategy)

- **achieves desired security outcomes** through ensuring industry participants in the transport sector are subject to similar legislative requirements, creating consistency in security requirements across Australia’s critical infrastructure sectors
- **supports coordination and collaboration** between government and industry, to enable an agile response to incidents where possible and appropriate.

The department has previously consulted aviation and maritime industry participants between March and May 2023, February 2024, and between May and July 2024 on components of the reforms considered in this IA. This consultation period followed an Independent Review of Australia’s Aviation and Maritime Security Settings (the Independent Review) that was delivered to government July 2022 recommending the legislative and policy frameworks be updated to enable iterative, risk-based, and scaleable regulation, as well as opportunities to improve government and industry capability and partnerships.

This IA argues that two problem elements exist in relation to the transport security legislative frameworks as outlined below.

*Table 1: Problem elements and government objectives*

What is the problem?		What are government’s objectives?
1.1.1	There are a growing number of threats to Australia’s transport sector, including an increasing risk of cyber incidents	<ul style="list-style-type: none"> <li>• Ensure government and industry are equipped to respond to current and emerging threats</li> </ul>
1.1.2	The dynamic and uncertain nature of these threats means the transport sector faces challenges in preparing for, mitigating, and responding to the realisation of these threats	<ul style="list-style-type: none"> <li>• Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards threats</li> <li>• Ensure Australia is proactive and adaptive to evolving international aviation and maritime security obligations</li> </ul>

This IA considers the regulatory impacts of four broad policy options to solve the problem identified in Table 1.

- **option 1:** maintain the status quo
- **option 2:** encourage industry to voluntarily uptake all hazards risk management
- **option 3:** switch on Critical Infrastructure Risk Management Program (CIRMP) obligations for ‘critical aviation assets’ and ‘critical ports’ under the *Security of Critical Infrastructure Act 2018* (SOCI Act) or
- **option 4:** amend ATSA, MTOFSA and their associated regulations to enact mandatory obligations.

Following analysis of the options, including consideration of which option would best achieve the government's objectives, the associated costs and benefits, and industry feedback, Option 4 has been identified as the preferred option.

The costs and benefits of all four options are assessed in this IA by considering a mixture of cost quantification (where possible) and evaluation of actual or hypothetical case studies (where the cost impact was uncertain or highly variable in magnitude and frequency). In assessing the costs and benefits of the proposed reforms, the marginal impact of each option on industry was considered. The specific marginal costs and benefits associated with each option is summarised below and is detailed in section 4.

To support the analysis, a Computable General Equilibrium (CGE) modelling approach was used to consider the direct and indirect impacts of the proposed changes to the broader economy where quantification of the impact of the reforms was possible. This approach modelled the economy as a system of interrelated economic agents operating in competitive markets. The modelling framework was appropriate for analysing the economic impact of a disruption to the aviation and maritime sectors as it explicitly captures supply chain linkages, and the flow-on effects both upstream and downstream of the incident.

To assess the benefits of the proposed reforms, this IA examined the potential disruptions arising from an all hazards security threat materialising. The avoidance of these potential events was the principal benefit expected from the proposed reforms, as disruption to the supply of goods and services, compromise of business operations, or other impacts can have a significant cost to the economy.

This IA identified the following costs and benefits for each of the four options:

**Option 1:** maintain the status quo:

- **Cost:** this option would see industry continuing to be exposed to threats and the increasing likelihood that an incident may occur as insufficient mitigations are in place. Section 4 provides case studies demonstrating the potential costs associated with the realisation of all hazard threats to which Australia's transport sector would continue to be exposed under option 1.
- **Benefit:** industry may benefit from ongoing operation in a familiar environment, with no additional regulatory requirements or costs.

**Option 2:** encourage industry to voluntarily uptake all hazards risk management:

- **Cost:** the effectiveness of voluntary uptake would vary depending on the degree to which entities choose to enhance their practices to address all hazard security threats. For industry participants who choose not to consider the guidance or implement recommendations distributed through various engagement forums, the costs incurred will be the same as those costs associated with option 1. These costs will be dependent on the severity and frequency of future all hazard security incidents.

- **Benefit:** variable benefits may arise and depend on the extent to which industry participants voluntarily choose to mitigate all hazard security risks. Industry will experience some of the benefits of avoiding future incidents depending on the extent of voluntary participation. The realisation of benefits is, however, inherently limited because participation is voluntary under option 2.

**Option 3:** switch on CIRMP obligations for 'critical aviation assets' and 'critical ports' under the SOCI Act:

- **Cost:** there may be additional costs to industry participants that are in scope to comply with the CIRMP obligations. Further, industry would have to respond to the security obligations across different legislative frameworks (SOCI Act vs. ATSA/MTOFSA), imposing additional costs. While the CIRMP framework will allow for a consistent increase in the risk management practices amongst certain transport sector entities, it does not reflect the diversified nature of the sector. Consequently, there will be a cohort of industry participants (such as tier 1 and 2 airports or ship operators) that are not required to identify and mitigate all hazards risks under this option.
- **Benefit:** there may be some benefit arising from option 3, where the application of the CIRMP obligations can contribute to the avoidance of incidents that may otherwise disrupt operation and lead to economic loss. However, this benefit will only extend to those industry participants captured under the SOCI Act, rather than creating a potential benefit for the whole of Australia's transport sector. Benefits would likely be greater than under option 2 but would be less than under option 4.

**Option 4:** amend ATSA, MTOFSA and their associated regulations to enact mandatory obligations:

- **Cost:** an anticipated one-off cost to industry of \$190 million and an ongoing cost of \$115 million per year across the aviation and maritime sectors is expected; however, it is anticipated that a proportion of these costs will likely be passed on to consumers. Further information can be found in section 4.5.
- **Benefit:** proactively addressing and mitigating risks and hazards would reduce the likelihood and severity of incidents and disruption to supply chains across the economy. The proposed reforms can address the material risks to Australia's transport sector through the adoption of the all hazards security framework for all regulated aviation and maritime industry participants. This would occur through legislative requirements, which are robust, fit for purpose, proportionate to an industry participant's unique operating environment and size and by facilitating a coordinated uplift in their compliance with relevant standards.

The likely benefits of option 4 will be at least (and are expected to be more than) the costs of the regulation. This is because the frequency and severity of all hazard threats for the transport sector is increasing. While some events of the magnitude described in this IA have previously been considered to represent the worst-case disruption scenarios in Australia, the increasing severity and frequency of similar incidents, particularly in the context of growing cyber security incidents represents a risk to the whole economy. The increasing frequency of incidents makes the benefits associated with option 4 more likely to exceed the anticipated costs over time.

This IA considers industry feedback previously collected on the costs and benefits associated with each of these options and will provide a further opportunity for discussion with industry. This engagement has provided a key input for informing decisions by government on the nature of potential reforms. Industry consultation to date is comprehensively discussed in question 5. Implementation considerations and associated risks are discussed in question 7.



## Introduction

### Purpose of this document

This IA examines the costs and benefits associated with four potential options for reform to Australia's transport sector, comprising aviation, and maritime transport and offshore facility security legislation. The reforms discussed in this IA seek to strengthen the capabilities of the existing transport security legislative frameworks, through expanding the hazards which entities are required to plan for, mitigate, and respond to.

### Transport security legislative frameworks

The Australian Government must maintain legislation to safeguard the aviation and maritime sectors against unlawful interference. These are requirements of the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO) respectively. Ensuring Australia's legislation reflects the standards administered by ICAO and the IMO is one of Australia's international obligations.

Under the current legislative frameworks, the responsibility for managing the risk of unlawful interference is that of the entities which form part of Australia's transport sector. This includes a requirement that regulated entities mitigate terrorism, and serious crime.

### Aviation Transport Security Act 2004

The department regulates aviation security through ATSA and the *Aviation Transport Security Regulations 2005* (ATSR). The purpose of ATSA is to establish a legislative framework which safeguards against unlawful interference with civil aviation and to enforce aviation security, including the protection of air navigation, airport facilities, aircraft, and personnel.

ATSA provides a framework for entities to meet Australia's obligations under Annex 17 to the Convention on International Civil Aviation administered by ICAO. Annex 17 establishes standards that must be implemented by contracting states and recommends best practices to do so.

ATSA also requires regulated aviation industry participants to submit a security program to the department which sets out the measures and procedures regulated entities are required to implement to mitigate security risks.

### Maritime Transport and Offshore Facilities Security Act 2003

The department regulates maritime transport and offshore facility security through MTOFSA and the *Maritime Transport and Offshore Facilities Security Regulations 2003* (MTOFSR). MTOFSA supports Australia in meeting its obligations under Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS) and the International Ship and Port Facility Security Code (ISPS Code).

The SOLAS and the ISPS Code establish an international framework between contracting governments and the maritime industry, which aims to detect security threats and deter acts of unlawful interference and organised crime that threaten the security of ships and port facilities used in international trade.

MTOFSA requires certain maritime industry participants to submit a security plan to the department which sets out the measures and procedures regulated entities are required to implement to mitigate security risks.

Security programs and plans will be referred to collectively as security programs throughout this IA unless specified otherwise.

### **Security of Critical Infrastructure Act 2018**

The SOCI Act introduces security obligations for the owners and operators of captured critical infrastructure assets. These include requirements to:

- report information (such as operational information or interest and control information) to the Register of Critical Infrastructure Assets
- report cyber incidents
- develop a CIRMP, to identify and mitigate all hazards risks
- notify any data service providers whether they hold business critical data on behalf of a critical infrastructure asset
- comply with cyber incident response government assistance measures.

Under the SOCI Act, captured critical infrastructure entities are required to proactively identify and mitigate all hazards, including:

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

'Critical aviation assets'<sup>2</sup> and 'critical ports'<sup>3</sup> are subject to different security obligations under the SOCI Act, as demonstrated in table 2 below. Neither asset class is required to maintain a CIRMP.

The department also administers the SOCI Act. The SOCI Act applies to 11 sectors of critical infrastructure and 22 asset classes, including 'critical aviation assets' and 'critical ports'. The SOCI Act aims to strengthen the security and resilience of critical infrastructure.

---

<sup>2</sup> Assets that are: used in connection with the provision of an air service and owned or operated by an aircraft operator; used in connection with the provision of an air service and is owned or operated by a regulated air cargo agent; used by an airport operator in connection with the operation of an airport.

<sup>3</sup> Broome Port; Port Adelaide; Port of Brisbane; Port of Cairns; Port of Christmas Island; Port of Dampier; Port of Darwin; Port of Eden; Port of Fremantle; Port of Geelong; Port of Gladstone; Port of Hay Point; Port of Hobart; Port of Melbourne; Port of Newcastle; Port of Port Botany; Port of Port Hedland; Port of Rockhampton; Port of Sydney Harbour and Port of Townsville.

**Table 2: Transport Security obligations under the SOCI Act**

Asset	Register of critical infrastructure assets	Obligation to report cyber incidents	Obligation to develop a CIRMP	Obligation to notify data service providers
<b>Critical aviation assets</b>		√ <sup>4</sup>		√
<b>Critical ports</b>	√	√		√

Critical aviation assets and critical ports are not subject to the obligation to maintain a CIRMP because of their existing security program obligations under ATSA and MTOFSA (with the exception of some critical liquid fuel assets also regulated under MTOFSA). The security program obligations currently require greater detail but only cover physical and personnel security risks. The CIRMP mandates cover the five all hazard security domains. This is a reflection of the problem identified in this IA, and must be considered when assessing options to address it.

**Development of this IA**

The department engaged closely with the Office of Impact Analysis (OIA) as it considered potential options for addressing identified gaps in the regulation of Australia’s transport sector. This engagement will continue throughout the policy development process. This IA is being developed concurrently to key stages in policy development, outlined below.

The analysis contained in this document will continue to evolve alongside policy development, as per table 3.

**Table 3: Policy development process**

Policy Development State	IA development Stage
Consultation on the nature of the proposed reform measures for industry	Early Assessment IA
Decision by government to implement proposed reform measures	First Pass IA
Final decision by government to implement proposed reform measures	Second Pass IA

<sup>4</sup> This obligations applies to a smaller subset of aviation assets, being: a designated airport; an Australian prescribed air service operating screened air services that depart from a designated airport, or a regulated air cargo agent that is also a cargo terminal operator at a designated airport

# 1. What is the policy problem you are trying to solve and what data is available?

Australia's transport sector is crucial for connecting Australians with critical goods and services, and allowing for transportation across the world. The interconnected nature of critical infrastructure, including aviation and maritime entities, means that any disruption to any industry participant's operations or its supply chains can have cascading effects on dependent infrastructure and networks. If destroyed, degraded, or rendered unavailable for an extended period, Australia's security, economic position and overall prosperity may be significantly impacted.

There has been a considerable shift in the global threat environment. This includes increases in the scale and frequency of attacks on the Australian transport sector which will continue to impact Australia's national security across a range of hazard domains such as physical, natural hazard, supply chains, personnel, and cyber.

The evidence of the deteriorating risk environment within the transport sector is substantial. While many of the studies and data relates to the overseas experience, the interconnected nature of the transport sector (through transport connections, global ownership structures or shared global trends in operations) makes it relevant for the Australian transport sector. For example, the global trend toward greater use of internet-connected operating technology in the maritime environment increases security risks for both Australian and overseas entities adopting these technologies.

In the aviation sector, the following global trends have been observed:

- ICAO reported that cyberattacks on the aviation industry increased 24% worldwide in the first half of 2023. Persistent passive attacks (including port scans, pings and traffic monitoring) are allowing attackers to discover open ports and protocols<sup>5</sup>
- Across the European aviation sector, European Air Traffic Management observed a steady increase in new cyber security incidents during 2023. Compared with 2022, there was nearly three times as many new cyber security incidents within the sector.<sup>6</sup>

In the maritime sector, similar trends are demonstrable:

- In June 2024, the World Economic Forum reported that since 2020, over 80% of world transport leaders have increased investments in information technology (IT) and OT. This investment introduces a higher level of cyber risk, demonstrated by a 456% increase in maritime sector organisations that have paid a ransom in the year to June 2024.<sup>7</sup>

---

<sup>5</sup> Cyber Security and Resilience Symposium, ICAO, 2023, <http://www.icao.net/cybersecurity-and-resilience-symposium-presentation>, p. 7

<sup>6</sup> Update on ground handling matters, European Air Traffic Management, ERAA, 2024 [www.eraa.org/update-ground-handling-matters](http://www.eraa.org/update-ground-handling-matters)

<sup>7</sup> World Economic Forum, 2024, [www.weforum.org/transport-supply-chain-resilience](http://www.weforum.org/transport-supply-chain-resilience)

- In 2023, the United States Coast Guard reported an 80% increase in ransomware incidents targeting the maritime sector from 2022 to 2023. These incidents targeted maritime shipping companies, liquid natural gas processors and distributors, petrochemical companies, and maritime logistics and technology service providers.<sup>8</sup>

While security measures historically applicable to both aviation and maritime industry participants have been focused on mitigating and responding to terrorism-related issues, we now see espionage, foreign interference, cyber security threats and other events captured by all hazards expanding in their prominence, frequency, and severity. These threats include:

- **An ongoing risk of interference by sophisticated insiders** who may exploit their access to secure airport and port facilities to cause disruption or engage in criminal activity. For example, on 11 June 2021, an insider working for an Australian air services company was arrested, as part of Operation Ironside, which targeted organised crime syndicates, and was charged with drug trafficking and money laundering offences<sup>9</sup>
- **An observed increase across Australia’s critical infrastructure in the number of cyber incidents.** In 2022-23, the Mandatory Cyber Incident Reporting regime for critical infrastructure assets identified that there were 188 significant or relevant incidents impacting Australia, with flow on impacts related to the confidentiality, integrity or reliability of Australian critical infrastructure<sup>10</sup>
- For the transport sector, **a traditionally narrow approach to regulating security** (focused on terrorism and serious crime) can leave open the realisation of threats arising from broader security risks, such as those related to espionage and foreign interference, cyber security and insiders.<sup>11</sup>

Additionally, the Royal Australian Navy has identified the global maritime sector is increasingly digitalised, automated, and connected, increasing its vulnerability to cyber threats.<sup>12</sup>

More broadly, natural hazard incidents (including catastrophic floods in parts of Australia and the global COVID-19 pandemic) have highlighted vulnerabilities in Australia’s critical infrastructure and supply chain resilience. In relation to the pandemic:

*“COVID-19...highlighted Australia’s dependency and exposure to overseas markets and events. The collated risk of this dependency has never been contemplated by industry or governments, prompting significant reactions and fast-thinking during the COVID-19 isolation period. Supply chain analysis, management and interrogation will need to become critical activities for Australian industry, changing the way industry have [sic] traditionally approached and managed supply chains to date.”<sup>13</sup>*

<sup>8</sup> Cyber Trends and Insights, US Coast Guard, 2023, [www.uscg.mil/cyber-trends-and-insights](http://www.uscg.mil/cyber-trends-and-insights) p. 13

<sup>9</sup> Airport worker arrested for drug trafficking, The Sydney Morning Herald, 2021, [smh.com.au/airport-worker-arrested-charged-with-drug-trafficking](http://smh.com.au/airport-worker-arrested-charged-with-drug-trafficking)

<sup>10</sup> 2023–2030 Australian Cyber Security Strategy, [homeaffairs.gov.au/cyber-security-strategy-legislative-reforms](http://homeaffairs.gov.au/cyber-security-strategy-legislative-reforms), p. 33

<sup>11</sup> Safe Shipping: A forgotten aspect of maritime security, Australian Strategic Policy Institute, 8 November 2023, [aspistrategist.org.au/safe-shipping-a-forgotten-aspect-of-maritime-security-in-the-pacific](http://aspistrategist.org.au/safe-shipping-a-forgotten-aspect-of-maritime-security-in-the-pacific)

<sup>12</sup> Royal Australian Navy, 2021, [seapower.navy.gov.au/media-room/publications/soundings-42](http://seapower.navy.gov.au/media-room/publications/soundings-42)

<sup>13</sup> Defence Teaming Centre, Submission 61, [aph.gov.au/implications-of-covid-19/supply-chain-integrity](http://aph.gov.au/implications-of-covid-19/supply-chain-integrity), p. 3

For the transport sector, the sudden and ongoing impact of the pandemic demonstrated Australia’s existing reliance on single-source international delivery systems.

The United Nations’ Intergovernmental Panel on Climate Change (IPCC) has reported that natural disasters fuelled by the climate change will continue to intensify.<sup>14</sup> These hazards have and will cause, widespread and substantial impacts, losses and damages, including potential damage to infrastructure, coastal areas (including low lying port infrastructure) and damage to key economic sectors.<sup>15</sup> Specifically, the IPCC provides:

*“Urban infrastructure, including transportation, water, sanitation, and energy systems have been compromised by extreme and slow-onset events, with resulting economic losses, disruptions of services and negative impacts to well-being.”<sup>16</sup>*

The unpredictability and unprecedented nature of these events, and their impact on the security and stability of critical infrastructure entities, creates a need to strengthen Australia’s existing transport security legislative frameworks.

Currently, the limited focus of ATSA, MTOFSA and their associated regulations (which are restricted to requirements to mitigate the threat of unlawful interference within designed boundaries) does not reflect the current security environment nor the range of risks which currently face Australia’s transport sector.

## 1.1 Problem Elements

This First Pass IA considers two key problem elements, which currently impact the transport sector, including the ability for maritime and aviation industry participants to prepare for, prevent and respond to all hazards threats.

*Table 4: Overview of problem elements*

Problem elements	
1.1.1	There are a growing number of threats to Australia’s transport sector, including an increasing risk of cyber incidents
1.1.2	The dynamic and uncertain nature of these threats means the transport sector faces challenges in preparing for, mitigating and responding to the realisation of threats

These problem elements are analysed in further detail below.

<sup>14</sup> Climate change synthesis report, Intergovernmental Panel on Climate Change, 2023, [www.ipcc.ch/climate-change-synthesis-report](http://www.ipcc.ch/climate-change-synthesis-report) p. 7

<sup>15</sup> Climate change synthesis report, Intergovernmental Panel on Climate Change, 2023, [www.ipcc.ch/climate-change-synthesis-report](http://www.ipcc.ch/climate-change-synthesis-report) p. 7

<sup>16</sup> Climate change synthesis report, Intergovernmental Panel on Climate Change, 2023, [www.ipcc.ch/climate-change-synthesis-report](http://www.ipcc.ch/climate-change-synthesis-report) p. 6

### 1.1.1 There are a growing number of threats to Australia's transport sector

Government and industry must contend with protecting Australians against a broad spectrum of threats and hazards. The security and resilience of Australia's critical infrastructure faces potential threats across 5 hazard domains (summarised in table 5 below), each of which have the potential to cause significant disruption across the Australian economy.

The department leverages industry knowledge of the different sectors, businesses, operations and processes to understand the environment and approach to increasing capability, and to collaboratively ensure the security, continuity and resilience of Australia's critical infrastructure. This includes an understanding that potential threats, including the risk of cyber security incidents, continue to increase. For example:

- During 2022–23, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) responded to 143 incidents reported by entities who self-identified as critical infrastructure. This is an increase from the 95 incidents reported in 2021–22.<sup>17</sup>
- ASD's ACSC responded to 79 cyber security incidents involving denial-of-service (DoS) and distributed denial-of-service (DDoS) in 2022-23, which is more than double the 29 incidents reported to ASD's ACSC in 2021-22.<sup>18</sup>

Many of the hazard domains and associated risk areas described in the table below have arisen or expanded in the 20 years following the initial enactment of the transport security legislative frameworks.<sup>19</sup> This expansion is also reflected in industry's operating environments, which have evolved to meet the growing demands of transport services across Australia and from the broader international community.

Australia's transport security legislative frameworks place a strong focus on mitigating the threat of unlawful interference, terrorism, and serious crime within a physical boundary, with no specific obligations on entities to protect their operations from cyber security incidents, supply chain disruptions or natural hazards. The transport sector faces an increasingly complex security environment, which make the problem elements in Table 4 of particular concern to both industry and government.

---

<sup>17</sup> Cyber threat report 2023, ASD's ACSC, 2023, [www.cyber.gov.au/cyber-threat-report-2023](http://www.cyber.gov.au/cyber-threat-report-2023)

<sup>18</sup> Cyber threat report 2023, ASD's ACSC, 2023, [www.cyber.gov.au/cyber-threat-report-2023](http://www.cyber.gov.au/cyber-threat-report-2023)

<sup>19</sup> Critical Infrastructure Annual Risk Review, CISC, 2023, [cisc.gov.au/critical-infrastructure-annual-risk-review](http://cisc.gov.au/critical-infrastructure-annual-risk-review)

**Table 5: Overview of the 5 hazard areas**

Hazard domain	Identified risk	Example
<b>Physical</b>	Physical hazards may disrupt the functioning of critical infrastructure and the systems that rely upon its function. This may include systems and networks which operate to protect from and mitigate the impacts of human induced threats	Threats of terrorism or piracy may attempt to disrupt physical facilities such as airports, seaports, or maritime vessels through acts of sabotage, hijacking or armed attacks posing risks to passengers and infrastructure. There are also risks of sabotage by malicious actors to critical infrastructure’s physical facilities
<b>Personnel</b>	Personnel with access to systems, data or premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data. This includes personnel such as employees, owners, operators, contractors, and subcontractors	In the transport sector, there has been a risk of issue-motivated disruptions perpetrated by insider personnel. <sup>20</sup> Issue motivated groups can create disruptions through cyberspace and via non-violent protests, as well as serious and organised crime groups concealing illicit commodities from authorities while in transit <sup>21</sup>
<b>Cyber</b>	Cyber threats can disrupt the digital systems, computers, datasets, and networks an organisation relies on. This can result in an ‘unintended taint’ (where software design or implementation flaws increase susceptibility to cyber risks) or ‘malicious taint’ (deliberate diversion or disruption to cyber supply chains)	Cyber security threats are outpacing terrorism threats. <sup>22</sup> DDoS attacks, fraudulent websites and emails, and ransomware attacks are of key concern for the transport sector
<b>Supply chain</b>	Supply chain risks include threats to organisations, people, activities, information, and resources that support Australia’s critical infrastructure and the delivery of essential goods and services. This risk is compounded where organisations are reliant on suppliers in a particular part of the world that may also experience supply chain disruptions	Australia’s transport sector acts as a gateway and point of connection to resources and services across other critical infrastructure sectors including energy, health care and services, and food and grocery. Disruptions to the transport sector can have significant impacts to the supply chains of other sectors <sup>23</sup>
<b>Natural hazard</b>	Natural hazards are unexpected or uncontrollable geophysical events, which have the potential to cause damage or loss to an organisation, its people, systems, or property	Climate change is a threat to transport infrastructure. Airlines and their pilots rely on predictable weather conditions to make crucial decisions to enable safe flights, and the maritime sector is vulnerable to sea-borne weather events due to its littoral nature. Natural hazards can cause up-stream supply chain outages that may affect the delivery of essential transport services

New technologies have resulted in the enhanced connectivity and complexity of transport operations. Large IT systems organise and sort data in quantities impractical to humans, and OT performs these outcomes autonomously. Such systems are critical to the coordinated operation of air and seaports, and link information and systems to operations.

<sup>20</sup> Critical Infrastructure Annual Risk Review ,CISC, 2023, [cisc.gov.au/critical-infrastructure-annual-risk-review](https://cisc.gov.au/critical-infrastructure-annual-risk-review)

<sup>21</sup> Trends and issues in crime and criminal justice, AIC, 2023, [aic.gov.au/trends-and-issues-in-crime-and-criminal-justice](https://aic.gov.au/trends-and-issues-in-crime-and-criminal-justice)

<sup>22</sup> Protective Security Policy Framework, AGD, [protectivesecurity.gov.au/protective-security-policy-framework](https://protectivesecurity.gov.au/protective-security-policy-framework)

<sup>23</sup> Transport and Supply chain ecosystems, World Economic Forum, 2024, [weforum.org/transport-and-supply-chain-ecosystems-increasingly-digitized-and-automated](https://weforum.org/transport-and-supply-chain-ecosystems-increasingly-digitized-and-automated)



In the aviation sector, international commercial travel has expanded exponentially since the 1970s, as depicted in by Figure 1 below. Despite the impact of COVID-19 and associated border closures on the demand for commercial air travel, the numbers of domestic and international travellers are slowly returning to pre-pandemic levels.<sup>24</sup> The aviation sector is experiencing advances in technology that could lead to greater increases in travel and freight volumes. These technologies could result in the further integration of OT with computer and IT systems.

**Figure 1: Revenue trends in international travel**



In the maritime context, the number of twenty-foot equivalent units (TEU) of containers moved through Australian ports grew 130% between 2000 and 2021.<sup>25</sup> This example of increased demand alone has resulted in a requirement for larger ships and increased maritime traffic in Australia.

The maritime sector has experienced changes to shipping traffic (as outline in table 6 below), creating challenges in maintaining a risk-based approach to compliance. For example, increased shipping traffic creates a need for additional resources to conduct inspections of foreign ships. These inspections are crucial for verifying compliance with international regulations and ensuring maritime safety and security.<sup>26</sup>

<sup>24</sup> Cyber Security and Resilience Symposium, ICAO, 2023, <http://www.icao.net/cybersecurity-and-resilience-symposium-presentation>, p. 7

<sup>25</sup> The World Bank, 2021, <https://databank.worldbank.org/source/world-development-indicators>

<sup>26</sup> World development indicators data series, The World Bank, 2021, [worldbank.org/world-development-indicators](http://worldbank.org/world-development-indicators)

Table 6: Ship arrivals data<sup>27</sup>

Ship Type	2020	2021	Change
Bulk Carrier	14,355	14,814	3.2%
Chemical tanker	1,555	1,370	-11.9%
Container ship	3,698	3,675	-0.6%
Gas carrier	1,474	1,406	-4.6%
General cargo/ multi-purpose	927	1,038	12.0%
Livestock carrier	351	281	-19.9%
Oil tanker	757	733	-3.2%
Vehicle carrier	1,274	1,524	19.6%
Other	1,847	1,559	-15.6%
<b>Total Arrivals</b>	<b>26,179</b>	<b>26,400</b>	<b>8.4%</b>

Technological advancements have been a key mechanism through which the transport sector has sought to expand the demand for its services. This has resulted in an increased reliance on legacy systems and internet connected OT. In reporting on key trends in the maritime environment, the US Coast Guard observed the following in relation to OT:

- OT networks often contain an organisation’s most critical and vulnerable systems
- OT systems often use vulnerable network protocols, making them a target for potential cyber security incidents
- these risks are exacerbated where OT systems lack adequate access controls, allowing malicious actors’ access to both IT and OT systems.<sup>28</sup>

These risks indicate a need for modern legislative regimes which can capture technological advancements and ensure the uptake of technology which delivers benefits to the Australian economy. More broadly, the evolution of Australia’s transport sector means there is a need for ongoing review and where appropriate, reform, to ensure Australia’s legislative and regulatory transport security arrangements are fit-for-purpose and capable of meeting security objectives.

Where legislation does not respond to the growing number of threats which are facing Australia’s transport sector, disruptions can have serious implications for businesses, governments, and the community. These disruptions create flow-on affects to the security of resources, supply, and service continuity, and damage our economic growth. Table 7 below provides a summary of these potential impacts.

<sup>27</sup> Port State Control Annual Report, Australian Maritime Safety Authority, 2021, [amsa.gov.au/port-state-control-australia-annual-report-2021](https://amsa.gov.au/port-state-control-australia-annual-report-2021)

<sup>28</sup> Cyber Trends and Insights, US Coast Guard, 2023, [www.uscg.mil/cyber-trends-and-insights](https://www.uscg.mil/cyber-trends-and-insights) p. 13

Table 7: Summary of stakeholder impacts from growing threats

Stakeholder group		Relationship to hazards in the transport sector	Impact
Industry		Responsible for mitigating and affected by all hazards	If a security incident significantly impacts the service delivery of essential goods and services, an industry participant may bear the burden of reputational risk, financial loss, legal consequences, the leak of sensitive data and potential punitive measures from the regulator. There are costs associated with replacing damaged infrastructure and operational disruptions for industry, and the costs for both industry and the public with the loss of assets essential for travel and trade
Government	<i>Local</i>	Responsible for managing and minimising risks to continuity in the event of any disruption	Local, state, and federal governments are expected to mitigate threats to the Australian community and may face criticism and reputational damage when seen to be inadequately responding to security incidents
	<i>State and Territory</i>		
	<i>Federal</i>	Develop, align and regulate legislation to ensure industry is appropriately protected	
	<i>Foreign governments</i>	Affected by supply chain issues	
Community		Affected by all hazards	Natural and man-made disruptions to the transport sector could have large consequences on the Australian community and general public, from inaccessibility to essential goods and travel disruptions to financial loss and the loss of sensitive personal data. In extreme cases, incidents could result in serious injury or death

## 1.1.2 The dynamic and uncertain nature of threats creates challenges for the transport sector

The scale, frequency and complexity of cyber threats, sophisticated foreign intelligence service activities against Australian interests, as well as natural hazards such as bushfires and floods, are increasing.<sup>29</sup> The nature of these threats means they are surpassing the security and resilience mechanisms within the transport security legislative frameworks. These threats include potential impacts arising from physical and natural hazards (such as fires, floods, cyclones, and health hazards).

The below case studies explore these threats in further detail.

DP World cyber-attack (2023) <sup>30</sup>	Cyber Supply chain
--	-----------------------

**Situation:** DP World, a major logistics company with operations in Australia, experienced an interruption at 4 of its Australian container terminals due to an exploited vulnerability in the company's IT systems. To limit the spread of the breach once detected, the operator disconnected all on-land networks, resulting in an inaccessible landside area for freight vehicles.

**Outcome:** The affected container terminals are responsible for 40% of Australia's imports and exports. Operations were disabled for several days. Over this period, some 30,000 twenty-foot equivalent units of containers were idle across the country. The outage resulted in many sectors and consumers having been negatively impacted by the downstream supply chain consequences associated with the affected terminals.

**Identified gap:** The vulnerability exploited in this circumstance was a well-known bug in the operator's Citrix software. The patch to fix this bug was available to the operator but had not yet been installed. This case study demonstrates that entities should prioritise implementing cyber security mitigation strategies and programs to best protect themselves against a cyber incident.

---

<sup>29</sup> Critical Infrastructure Annual Risk Review ,CISC, 2023, [cisc.gov.au/critical-infrastructure-annual-risk-review](https://cisc.gov.au/critical-infrastructure-annual-risk-review)

<sup>30</sup> DP World data breach Reuters, 2023, [reuters.com/dp-world-data-breach](https://reuters.com/dp-world-data-breach)

## Cyber-attacks target aviation in groups (2022-23)<sup>31</sup>

Cyber

**Situation:** Recent trends show multiple aviation entities being targeted by cyberattacks simultaneously. Attacking aviation entities in targeted groupings disrupts the nation's aviation sector holistically. In 2023, airports in Canada experienced outages at check-in kiosks and electronic gates as the result of DDoS attacks. In the United States in 2022, 14 major airports had their websites disabled concurrently, and in Germany in 2023, seven airports experienced unanimous disruptions to the delivery of their information services.

**Outcome:** State sponsored actors claimed responsibility for all 3 incidents. In all 3 cases, operations were resumed on the day they occurred, and they caused no major one-off costs to the entity. However, all 3 circumstances resulted in delays or cancellations of flights towards or from the affected airports, creating a broader economic detriment to the nations they occurred within, as business and other people movements were disrupted.

**Identified gap:** Aviation entities are intrinsically interconnected both with each other and the functioning of a prosperous nation. Strengthening the resilience of the aviation sector to cyber threats can significantly reduce the consequences that might occur.

## Cyclone Jasper forces Cairns airport to close from floods<sup>32</sup>

Natural hazard  
Supply chain

**Situation:** In 2023, cyclone Jasper caused major destruction across north Queensland. Heavy rainfall and damaging winds of up to 90km/h meant that Cairns airport temporarily closed due to flooding, leaving several planes partially under water on the tarmac.

**Outcome:** Australia's tourism sector was impacted by an estimated loss of \$60 million due to holiday cancellations because of extreme weather. This impacted northern Queensland during peak tourist season at the start of the Australian summer. Severe weather conditions meant helicopter support, air transport and rescue services were not immediately available to assist local emergency services to respond. Cairns airport, through the use of documented emergency management processes and procedures, were able to restore critical air services for emergency response within 12 hours of the peak of flooding and recommence mainline commercial operations within 24 hours.

**Identified benefit:** This incident demonstrated the importance of emergency management planning for responding to a large-scale natural disaster. Proactive measures supported the aviation sector in minimising the extent and duration of supply chain issues (such as the flow on effects to critical emergency services) when it was rendered inoperable due to a natural weather event.

<sup>31</sup> CSIS, Significant Cyber Events List, 2024, [csis.org/significant-cyber-incidents](https://www.csis.org/significant-cyber-incidents)

<sup>32</sup> Cairns airport closure due to floods, Australian Financial Review, 2023, [afr.com/cairns-airport-closure-due-to-floods](https://www.afr.com/cairns-airport-closure-due-to-floods)

**Situation:** In 2018, malicious actors hacked the British Airways' website and app and stole data from approximately 430,000 customers (with 58% of these customers experiencing theft of their sensitive details).<sup>34</sup> The hackers accessed the airline's system by disguising themselves and entering through a different domain. The hackers then attached malware to the airway's browser, which was programmed to collect payment information fields when customers interacted with the website.

**Outcome:** The attack resulted in the compromise of customers' names, email addresses and credit card details (including card numbers, expiry dates and 3-digit CVV codes). In October 2021, Britain's Information Commissioner's Office fined British Airways GBP20 million (AUD38.7 million) for failing to protect the personal and financial details of its customers. A class action followed the incident, with a group of 23,000 (as at July 2021) claimants suggesting they incurred damages as a result of the hack.<sup>35</sup> While the details of the class action settlement are confidential, estimates suggest claimants may receive an average of GBP2,000 each (AUD3,908).<sup>36</sup> Based on these estimates, the total cost of the data breach to the airline was as much as AUD129 million in fines and compensation alone. This would not include any additional costs associated with strengthening cyber security (about which the airline made no public announcement).

Following this incident, 2020 saw 61% of all identified cyber-attacks in Europe target airlines, almost twice as many as the two next largest market segments combined.

**Identified gap:** This incident demonstrated a failure by British Airways to consider the risks of potential cyber-attacks and apply adequate protections for sensitive customer data. While this example is outside Australia, similar data breaches from cyber incidents have recently occurred in other critical infrastructure sectors in Australia (such as the Optus and Medibank breaches). This leaves open the possibility of a similar event occurring to one of Australia's commercial airlines, where appropriate risk management protocols are not in place.

These case studies demonstrate the varied, yet significant, impacts of disruptions to Australia's transport sector. While the range of legislation identified throughout this section may support industry and government in preparing for and responding to all hazard threats, analysis has identified several gaps which limit a stakeholders' ability to do so. Furthermore, they demonstrate the importance of planning for current and emerging threats within the Australian context. Modernising the transport security legislative frameworks will ensure evolving threats in the operating environment are considered and mitigated by industry. This is required to ensure Australia's robust and effective transport sector continues to support national and societal resilience, and Australia's prosperity.

<sup>33</sup> British Airways fined \$26 million, BBC, 2020, [bbc.com/british-airways-fined-due-to-data-breach](https://www.bbc.com/news/technology-55888888)

<sup>34</sup> British Airways data breach, Independent UK, 2021, [www.independent.co.uk/british-airways-data-breach](https://www.independent.co.uk/news/technology/british-airways-data-breach)

<sup>35</sup> British Airways class action settles, Herbert Smith Freehills, 2021 [www.herbertsmithfreehills.com/british-airways-class-action](https://www.herbertsmithfreehills.com/news/british-airways-class-action)

<sup>36</sup> British Airways data breach compensation, Independent UK, 2021 [www.independent.co.uk/travel/news-and-advice/british-airways-data-breach-compensation](https://www.independent.co.uk/news/technology/british-airways-data-breach-compensation)

## 2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured?

### 2.1 Government’s objectives

There are several specific objectives for government’s intervention in considering opportunities for reform. These objectives are aligned with the two problem elements identified in Section 1 (as set out in table 8 below).

*Table 8: Problem elements and corresponding government objectives*

	What is the problem?	What are government’s objectives?
1.1.1	There are a growing number of threats to Australia’s transport sector, including an increasing risk of cyber incidents	<ul style="list-style-type: none"> <li>• Ensure government and industry are equipped to respond to current and emerging threats</li> </ul>
1.1.2	The dynamic and uncertain nature of these threats means the transport sector faces challenges in preparing for, mitigating, and responding to the realisation of these threats	<ul style="list-style-type: none"> <li>• Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards threats</li> <li>• Ensure Australia is proactive and adaptive to evolving international aviation and maritime security obligations</li> </ul>

With these objectives in mind, 4 policy options have been formulated. Each of these are discussed in detail in Section 3. These objectives have also been used to evaluate each option in question 6, and inform the development of potential indicators of success in question 7.

There may be some barriers to government achieving the objectives outlined above, which include:

- **resource barriers**, within industry and government, including financial and personnel constraints which may impact the ability to quickly respond to current and emerging threats
- **governance and policy barriers**, such as the processes and procedures required to be followed to support government intervention and allow government to achieve its objectives
- **stakeholder environment barriers**, including levels of trust between industry and government, which may influence industry’s level of willingness to collaborate with government.

Despite these potential barriers, government's existing strong relationship with industry and broader commitment to the security of Australia's aviation and maritime sectors means there is a strong likelihood that government intervention will achieve its desired objectives.

## 2.2 Why should government intervene?

Section 1 has highlighted the existing gaps in the transport security legislative frameworks which, without action, may make Australia's transport sector vulnerable to increasing all hazards risks posed by cyber incidents, supply chain disruptions, and natural hazards. There is an expectation from the Australian public that both industry and government are equipped with the right tools to support the preparation for, prevention of, and recovery from an all hazards incident.

The threat environment gives rise to a need for government to intervene to ensure the transport security legislative frameworks:

- **operates on a flexible, risk-based, and scalable basis**, ensuring obligations are adaptable and flexibly applied to entities based on their specific operating environments and size
- **holistically addresses potential vulnerabilities** that could have a relevant impact on aviation and maritime entities and flow-on effects for Australia's critical infrastructure, which will result in security requirements that support delivery of dynamic, modernised transport security legislative frameworks
- **achieve desired security outcomes** by ensuring industry participants are subject to the same legislative powers, creating consistency in security requirements and understanding across the transport sector
- **support coordination and collaboration between government and industry**, to enable an agile response to incidents where possible and appropriate.

Government maintains a unique ability to regulate across supply chains and on a whole-of-sector basis and can intervene to ensure vulnerabilities in critical infrastructure are proactively prevented, detected, and resolved. This is imperative for mitigating the potential impacts of disruption on Australia's social and economic stability, defence, and national security, as well as the reliability and security of other non-transport related critical infrastructure assets<sup>37</sup>. Government also holds primary responsibility for regulating Australia's critical infrastructure including, where possible, working in partnership with industry to ensure regulated entities understand and manage their own risk.

---

<sup>37</sup> Srinivas, J et al. Government regulations in cyber security: Framework, standards and recommendations. <https://www.sciencedirect.com/science/article/abs/pii/S0167739X18316753>



Government's established mechanisms for industry engagement, cooperation, and compliance support government intervention moving forward and primarily focus on ensuring all hazard security risks are appropriately managed:

- **Critical Infrastructure Resilience Strategy (CIRS)** provides a national framework for guiding Australia to enhanced critical infrastructure security and resilience. The CIRS includes an overarching vision for critical infrastructure, the impacts of changes in operating environments on critical infrastructure, and points of alignment between the CIRS and existing work across government, to enable achievement of objectives.<sup>38</sup>
- **Trusted Information Sharing Network (the TISN)** is government's primary tool for sharing business-government information sharing and resilience-building initiatives on critical infrastructure. The TISN provides a platform for industry and government representatives to share information that enhances mutual understanding and application of organisational resilience and contribute to achievement of the CIRS.<sup>39</sup>
- **Cyber and Infrastructure Security Centre (CISC)**, responsible for regulating the existing all hazards critical infrastructure regime, indicating government's commitment to working with asset owners and operators through engagement, partnerships, advice, risk assessments, exercises, modelling and regulation.<sup>40</sup>

In addition, government's continued involvement with critical infrastructure matters through the review and amendment of the applicable regulatory regime, aligns with each of the key objectives in the CIRS, including to:

- support critical infrastructure owners and operators to effectively manage risks to the continuity of their operations through mature risk-based and resilient approaches
- deliver initiatives through strong industry-government partnerships
- support critical infrastructure owners and operators to strengthen their security and resilience through regulatory frameworks, tools and improved collaboration.

The government is remaining vigilant against evolving threats through mechanisms of intervention in the transport sector. These mechanisms are essential to protect lives, safeguard our critical infrastructure assets, and ensure that the legislative and regulatory environment guiding the sector is efficient in allowing for the secure movement of people and goods domestically as well as beyond Australian borders.

While self-regulation by industry has been considered as an alternative to government action, the nature of the transport sector means it is not viable in this case. This is because:

- to be effective, regulation of the aviation, air cargo, and maritime sectors must be consistent (including the regulatory standards to which industry participants are expected to meet)

---

<sup>38</sup> Critical Infrastructure Resilience Strategy, CISC, 2023, [cisc.gov.au/critical-infrastructure-resilience-strategy](https://cisc.gov.au/critical-infrastructure-resilience-strategy)

<sup>39</sup> Trusted Information Sharing Network, CISC, 2024, [cisc.gov.au/trusted-information-sharing-network](https://cisc.gov.au/trusted-information-sharing-network)

<sup>40</sup> CISC, About Us, 2024, [cisc.gov.au/about-us](https://cisc.gov.au/about-us)

- self-regulation by industry may lead to inconsistent approaches across the transport sector and impact on its overall security.
- Australia is a signatory to international conventions of ICAO and the IMO, which seek to ensure the security of civil aviation, port facilities and ships.

Therefore, ongoing government intervention through government's ability to regulate on a whole of sector basis is the most likely means through which major security incidents are minimised and overall disruptions to the transport sector are mitigated.

### **2.3 Measures of success**

Measuring the success of government intervention is a key tool for allowing government to communicate its chosen regulatory approach to Australians. The established objectives of government can provide a lead into measures of success for government action reforming the transport security legislative frameworks. In achieving these objectives government will maintain the metrics described in table 9 below as measures of success.

Table 9: Framework for scenario development and sensitivity analysis

Relative importance	Measure of Success	Success factor/Key assumptions	Likelihood of applicable measurement
1	<p><b>Transport security legislative frameworks are robust, proportionate, and fit-for-purpose:</b> This means the legislative frameworks, including the policy settings for the transport security program frameworks, and the compliance and enforcement frameworks support government and industry participants to meet security objectives.</p>	<p>The reforms' success will be measured through the Government's ability to regulate in a flexible, scalable, risk-based way, and government and industry's resilience to current and emerging threats. This will be measured by industry's compliance with the frameworks and the minimisation of major security incidents and disruptions to Australia's transport sector.</p>	<p>High – Government will ensure the transport security legislative frameworks remain effective through regular review mechanisms, consideration of international best practice, regular engagement with industry, and an understanding of the threat environment.</p>
2	<p><b>Major security incidents in the Australian transport sector are minimised.</b> To the extent that it is avoidable, government will seek to ensure that Australian transport is enduringly safe and secure against the risks it faces currently and in the future.</p>	<p>The reforms' success will be measured by the extent to which the occurrence of major security incidents in the Australian transport sector are avoided. This objective will be measured based on the number of incidents over time and through the comparison between the number of major incidents in Australia and those that occur overseas.</p>	<p>Certain - Government will have oversight of all security incidents and can verify the secure operation of the transport sector</p>
3	<p><b>Disruptions to Australian transport operations caused by lapses in security are minimised.</b> Government, industry and the Australian public all benefit significantly from a reliable, consistent and predictable Australian transport sector that is safe from anything with the intent or capability to disrupt it.</p>	<p>The reforms' success will be measured by the extent to which the magnitude of security incidents when they do occur in the Australian transport sector are minimised or mitigated. This objective will be measured based on the magnitude of incidents in Australia over time and through the comparison between the scale of incidents in Australia and those that occur overseas.</p>	<p>High – Government has visibility over disruptions to transport sector operations that are the result of security lapses</p>

In pursuing its objectives, government must overwhelmingly maintain these metrics or success will not be achieved in its role as the regulator of transport security. These indicators are discussed further in question 7.

# 3. What policy options are you considering?

The department has identified 4 broad policy options in response to the identified problem elements:

- **option 1:** maintain the status quo
- **option 2:** encourage industry to voluntarily uptake all hazards security risk management
- **option 3:** switch on CIRMP obligations for 'critical aviation assets' and 'critical ports' under the SOCI Act
- **option 4:** amend ATSA, MTOFSA and their associated regulations to enact mandatory obligations.

Each option is described in detail below, including implementation considerations as applicable.

## 3.1 Option 1: Maintain the status quo

Option 1 involves no regulatory action or legislative change to ATSA, MTOFSA or the broader regime to address all hazard security threats and holistically consider and mitigate the risks industry participants their business operations. Existing legislation, regulations, standards, and guidelines relating to critical infrastructure would remain.

Under the status quo, transport sector industry participants primarily be obligated to consider the security risks posed by terrorism, serious crime and trusted insiders based on their physical premise. This requires entities to:

- maintain a security program that sets out the measures and procedures entities are required to implement to mitigate security risks
- report security incidents
- comply with directions under ATSA and MTOFSA
- implement additional security measures to secure zones and areas.

In this option, the pre-established problem elements will endure, and government will have limited capability to address the risks that Australia's transport sector faces.

### 3.2 Option 2: Voluntary uptake of all hazards security

Option 2 involves maintenance of the status quo while encouraging industry to voluntarily address all hazard threats and holistically consider and mitigate the risks facing their business operations.

This voluntary engagement would occur through:

- distribution and use of risk assessment materials and threat and hazard information, including sector specific intelligence-led risk assessments of critical incident pathways applicable to the transport sector, detailing the likelihood and consequence of security incidents that may lead to disruptions
- implementation of various measures and procedures, based on risk assessments including reference to specific standards or frameworks, for example, the Essential Eight Maturity Model from ASD's ACSC.

The CISC leverages partnerships across critical infrastructure sectors and between other government regulators and agencies to empower critical infrastructure owners and operators to remain resilient in an ever-changing risk and operating environment. This CISC also actively assists Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory requirements for the shared benefit of all Australians<sup>41</sup>. This includes the provision of risk assessment materials otherwise restricted to government use to industry, with the intention of allowing industry to better manage the threats facing critical infrastructure assets.

The department would use existing industry engagement mechanisms to share information and advice on risks and hazards and associated mitigation considerations, including

- Aviation Security Advisory Forum (ASAF)
- Regional Aviation Security Advisory Forum (RASAF)
- Air Cargo Security Industry Advisory Forum (ACSIAF)
- Maritime Industry Security Consultative Forum (MISCF)
- Strategic Aviation Security Meeting (SASM)
- Trusted Information Sharing Network (TISN).

These forums occur bi-annually (with the exception of MISCF, which occurs three times each year) as well as ad-hoc when required. For example, the industry mechanisms mentioned would be used as platforms for the department to consult industry on relevant policy papers, international best practice guidance and threat information relating to aviation and maritime security.

---

<sup>41</sup> Critical Infrastructure Annual Risk Review ,CISC, 2023, [cisc.gov.au/critical-infrastructure-annual-risk-review](https://cisc.gov.au/critical-infrastructure-annual-risk-review)

### 3.3 Option 3: Switch on CIRMP obligations for 'critical aviation assets' and 'critical ports' under the SOCI Act

Under option 3, the CIRMP obligations would be switched on for 'critical aviation assets' and 'critical ports' under the SOCI Act. Industry participants would be required to develop and maintain a CIRMP to identify and mitigate cyber, supply chain and natural hazards.

A CIRMP is a written program that identifies and manages the material risks of hazards that could have a disrupting impact on a critical infrastructure asset<sup>42</sup>. Switching this obligation on for the transport sector would see critical aviation assets and critical ports, as they are identified in the SOCI Act, establish programs to identify, minimise and, if possible, eliminate all hazards security risks.

A small number of transport sector entities are regulated under the SOCI Act. For example, there are 9 airports regulated by the SOCI Act, compared to 115 regulated by ATSA as of October 2024, in addition to aircraft operators, registered air cargo agents, accredited air cargo agents and known consignors that are also regulated<sup>43</sup>. There are 20 critical ports within the remit of the SOCI Act, and as at January 2019, MTOFSA regulated the security of 65 ports, 213 port facilities and 42 Australian ships.<sup>44</sup>

Logistically, under this option critical aviation assets and critical ports submit an annual report within 90 days after each relevant financial year concludes. The annual report establishes that a CIRMP is in place, and that the entity is compliant with the rules established in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023. A CIRMP does not need to be submitted alongside the annual report, however, the CISC as the relevant regulator may request to view the CIRMP as part of a compliance audit. The CIRMP process would be separate from and in addition to the security program requirements under ATSA and MTOFSA, which focus on physical and personnel security risks, and would only be applicable to the most critical transport sector assets. Regulating the same entities under both the SOCI Act and either ATSA or MTOFSA may potentially introduce a dynamic where entities have split security obligation across two legislative regimes, and potentially duplicative obligations.

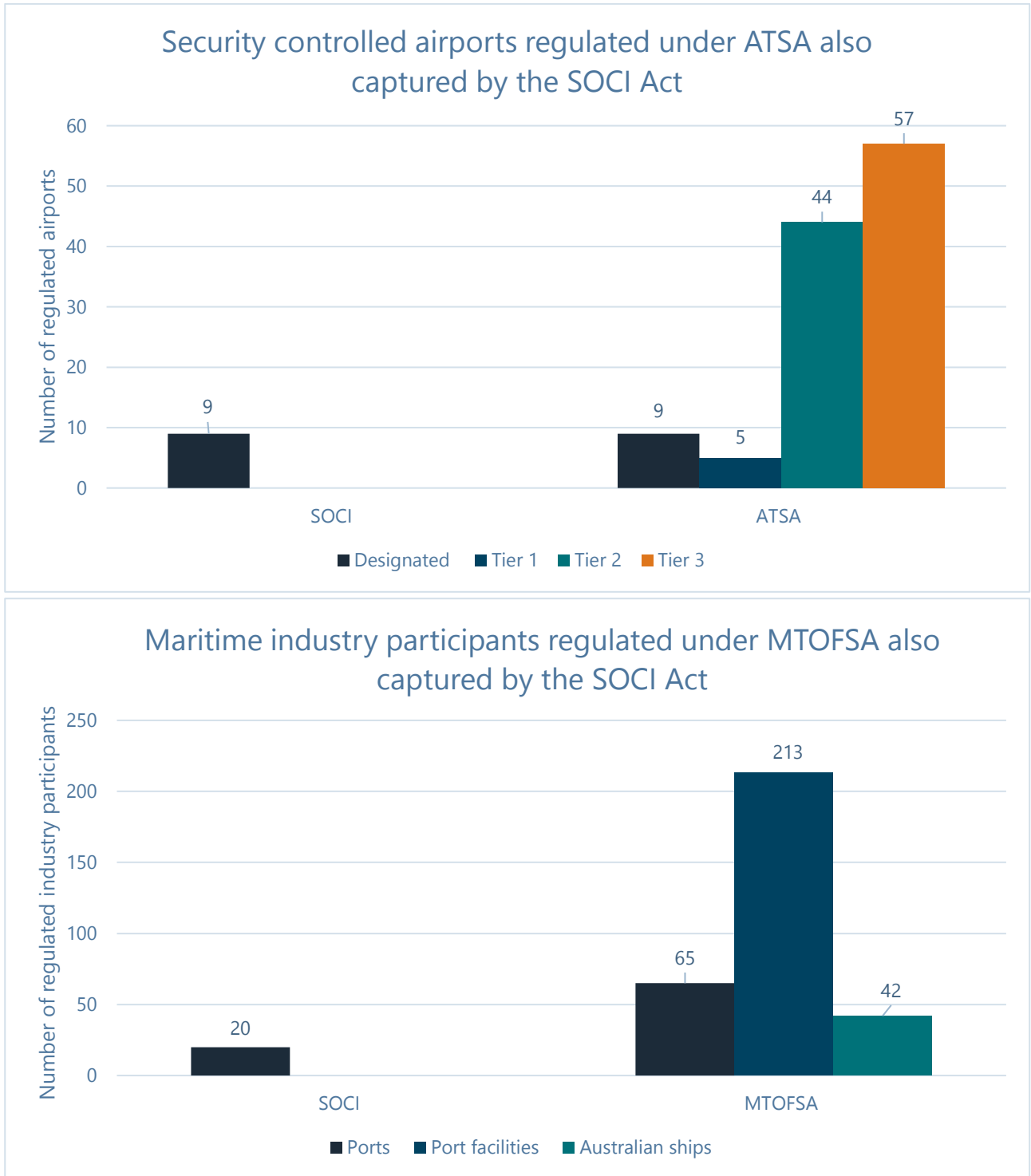
---

<sup>42</sup> Guidance for the critical infrastructure risk management program, CISC, 2024, [cisc.gov.au/guidance-for-the-critical-infrastructure-risk-management-program](https://www.cisc.gov.au/guidance-for-the-critical-infrastructure-risk-management-program)

<sup>43</sup> Federal register of legislation, 2024, [Notice Assigning Security Controlled Airport Category](#)

<sup>44</sup> Australian Parliament House, 2019. [aph.gov.au](https://aph.gov.au)

Figure 2: Capture of regulated aviation and maritime industry participants in the SOCI Act



### 3.4 Option 4: Amend ATSA, MTOFSA and its associated regulations to enact mandatory obligations

Option 4 seeks to amend the transport security legislative frameworks. The amendment will ensure that the aviation and maritime sectors can adapt and respond to current and emerging threats in a flexible, risk-based, and scalable manner. Option 4 comprises 15 measures, each of which have been grouped to support coverage and achievement of desired security objectives:

- **resilient to current and emerging threats** including measures that will strengthen the aviation and maritime sectors against all hazard threats, including cyber security
- **effective system testing program**, including measures that align with advances in technology, is risk-based and responsive to intelligence
- **robust compliance and enforcement framework** including measures that will create consistency, allow the regulator to have scalable options to address non-compliance, and will reflect the evolving and diverse threat environment and the introduction of the all hazards security framework and
- **modernisation and proportionate regulation** including measures that will remove elements of the transport security legislative frameworks, making it simpler for low-risk industry participants to meet requirements without reducing security outcomes.

The proposed measures are summarised in the table below and those which may result in a relevant cost impact are provided in full detail in Appendix A.

Consultation with industry on the first pass IA was held from 17 October to 24 October 2024. The department received 10 responses – five industry participants agreed with option 4 being the best option, 1 industry participant considered option 3 to be more reasonable and the remainder were unable or did not provide a view, citing additional information on what the obligations would be was needed to form a view. Further details of the outcomes of industry consultation are provided in section 5.2.3 below.



Table 10: Proposed measures

Measure	Summary	Affected sector
<b>Resilient to current and emerging threats</b>		
1. Unlawful interference	Expand the definition of unlawful interference and security incident reporting requirements to capture a variety of acts, including cyber security incidents	Aviation and maritime sectors
2. All hazards	Introduce all hazard security obligations. How the obligations apply to individual industry cohorts are outlined in Appendix B	Aviation and maritime sectors
3. Security controlled activities	Introduce a requirement for industry to identify and mitigate risks associated with personnel who have access to, or influence over, secure areas, or critical systems, remotely	Aviation and maritime sectors
<b>Effective system testing program</b>		
4. Test weapon definition	Amend the definition of test weapons to align with likely threat scenarios	Aviation sector
5. Vulnerability testing	Introduce vulnerability testing on Australian aviation and maritime security systems. Vulnerability testing involves a department officer acting as an adversary who has both the intent and capability to exploit a security system in an attempt to expose weaknesses. The proposed frequency and plan of vulnerability testing is not yet determined.	Aviation sector
6. Maritime systems testing	Introduce maritime system and vulnerability testing and provide Maritime Security Inspectors (MSIs) with equivalent protection and powers that Aviation Security Inspectors (ASIs) currently possess. A system test is designed to test a security screening system as a whole, including screening equipment and screening officers. These tests are used to determine whether the measures and procedures at a screening point are effectively implemented to detect weapons, and prevent their carriage into a secure area.	Maritime sector
<b>Robust compliance and enforcement framework</b>		
7. Special security directions (SSD)	Align SSD powers across ATSA and MTOFSA to enable it to be issued where there is a specific threat, or change in general threat or risk across all hazards. SSDs will continue to be exercised as a power of last resort.	Aviation and maritime sectors
8. Demerit points	Extend the demerit points system to the air cargo sector	Aviation sector
<b>Modernisation and proportionate regulation</b>		
9. Training requirements – Air Cargo	Allow training requirements for cargo-examining aircraft operators to be made through determinations to align with the rest of the air cargo sector	Aviation sector
10. Align authority for issuing security identification cards	Align the powers for authorising the charging fee for issuing a security identification card across the transport security legislative frameworks	Aviation sector
11. Amend definitions to secure Australia’s maritime ports	Amend the definition of ‘port’ and ‘security regulated port’ in the MTOFSA to allow the port boundary to be adjusted to capture areas that needs to be secured.	Maritime sector
12. Dual purpose vessels	Remove the requirement for ships that operate as both a ship and offshore facility to have two security plans	Maritime sector
13. Infrequent international vessels	Remove the requirement for a security plan for ships that infrequently travel internationally	Maritime sector
14. Gender	Replace ‘sex’ with ‘gender if practicable’	Aviation and maritime sectors
15. Remove reference to ‘fax’	Make the legislation technologically agnostic	Maritime sector

## 4. What is the likely net benefit of each option?

This IA focusses on identifying the broad categories of anticipated costs and benefits arising from the proposed policy options. A comprehensive scan has been conducted of available literature and evidence on the impacts of the options under consideration, including the potential benefits for individuals, businesses, government, community, and the economy, and the potential regulatory costs of each policy option. Ongoing consultation with industry on the potential reforms continues to provide valuable preliminary insights on the anticipated regulatory costs and benefits attached to each option.

This IA has analysed written submissions and outcomes from discussions with industry through consultation to:

1. validate the expected overall impacts and
2. better understand and quantify (where possible) the regulatory costs and benefits.

This IA considers the quantitative costs and benefits associated with option 4, using a breakeven analysis. Qualitative costs and benefits have been included to supplement this analysis. For option 1 (maintain the status quo), option 2 (voluntary uptake of all hazards risk management), and option 3 (switch on CIRMP obligations for critical aviation assets and critical ports) qualitative costs and benefits have been identified and analysed with quantification where possible.

### 4.1 Approach to determining costs and benefits

Costs will be identified by estimating the marginal impact on industry arising from the proposed reforms contained in options 3 and 4. Analysis will occur through a mixture of cost quantification (where possible) and evaluation of actual or hypothetical case studies (where the cost impact is uncertain or highly variable in magnitude and frequency). The specific marginal costs associated with each option is set out in the sections that follow.

The marginal impact of the proposed options will be borne by entities responsible for aviation and maritime security who meet the relevant thresholds. Community organisations and individuals are not likely to be directly affected, noting there may be indirect costs passed onto consumers. These indirect costs (flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents such as households and businesses) will be estimated using economic modelling based on the identified direct costs.

The benefits of each proposed measure will be identified through examination of potential disruptions arising from an all hazards security threat materialising. The avoidance of these potential events is the principal benefit expected from the potential reform proposals. Disruption to the supply of goods, compromise of business operations, or other impacts can have a significant cost to the economy. The interconnectedness between the transport sector and other sectors of critical infrastructure, including energy and healthcare and services, highlights how a disruption could have cascading implications.

The aim of the proposed reform options is to address the growing threats facing Australia's transport sector, including the uncertain and dynamic nature of potential incidents which have evolved since the initial introduction of the transport security legislative frameworks.

This IA analyses examples of all hazards events to demonstrate the potential direct and indirect (economy-wide) benefits which may arise from the avoidance of an incident. This analysis will reflect a real event with sufficient reliable information to substantiate estimated incident costs. The examples demonstrate the potential disruptions to the operation of the transport sector. They will consider incidents with varying severities because it may be the case that a series of smaller, less significant disruptions occur over the course of a year accumulate to deliver a resulting disruption equivalent to a severe scenario (e.g. the British Airways data breach which occurred in 2018). Consideration of the broader economic impact of an incident will also allow for identification of direct avoided costs (financial costs directly incurred because of an incident), as well as indirect avoided costs (flow-on costs to the economy).

For this IA, identified categories of costs associated with delay (for example, expenses and loss of income incurred as a result of an application or approval delay) as in the Australian Government's Regulatory Burden Measurement Framework<sup>45</sup> will not be considered. The proposed measures do not include a process which may delay the operations of new regulated entities.

## **4.2 Likely net benefit assessment: option 1 (status quo)**

This section summarises the qualitative costs and benefits associated with option 1, before assessing the likely net benefit derived from option 1.

### **4.2.1 Costs of option 1**

Option 1 provides a baseline for costs and benefits if the status quo is maintained and can be used as a comparator with the remaining three options. No additional regulatory measures would be imposed on industry participants. The most significant costs associated with option 1 are the transport sector's ongoing exposure to threats and the potential that an incident occurs and insufficient mitigations are in place. Maintaining the current transport security legislative frameworks may expose the government to reputational risk from both industry and the travelling public, as other critical infrastructure sectors are required to mitigate against a broader range of hazards.

---

<sup>45</sup> Regulatory burden measurement framework, OIA, 2024, [oia.pmc.gov.au/regulatory-burden-measurement-framework](https://oia.pmc.gov.au/regulatory-burden-measurement-framework)

Furthermore, option 1 does not address the international best practice relating to cyber security within the transport sector. For example, it would not consider:

- ICAO’s Cybersecurity Policy Guidance, or Standard 4.9.1 of Annex 17, requiring cyber security be a regulated component of aviation security
- the IMO’s Guidelines on Maritime Cyber Risk Management and the adoption of Resolution MSC.428(98) at its 98th session, which encourages governments to ensure cyber risks are appropriately addressed in existing safety management systems

For the purposes of modelling the potential costs associated with the realisation of all hazard security threats for Australia’s transport sector, the three scenarios noted in table 11 below were used. These scenarios and associated costs are based on case studies and analysis of real world disruptions arising from the realisation of all hazard threats. To support the analysis, a CGE modelling approach was used to consider the direct and indirect impacts of the proposed changes to the broader economy where quantification of the impact of potential all hazard incidents was possible. The case studies, associated costs and CGE modelling approach are discussed in greater detail in the section 4.5.2 below (discussion of option 4 benefits).

*Table 11: Summary of costs for each scenario*

	<b>Scenario 1 Port closure for 22.2 days (Severe)</b>	<b>Scenario 2 British Airways data breach (Moderate)</b>	<b>Scenario 3 50% of Moderate scenario (Low)</b>
Direct cost (\$ million)	\$291.5 million	\$129.0 million	N/A
Indirect cost (\$ million)	\$214.7 million	Nil *	N/A
Total cost to the economy of the incident (\$ million)	\$506.2 million	\$129.0 million	\$64.5 million

Without adequate protections, industry and the Australian economy as a whole may incur costs in line with these scenarios dependent on the severity and frequency of the disruption.

#### 4.2.2 Benefits of option 1

Under option 1, individuals and industry may benefit from ongoing operation in a familiar, consistent regulatory environment, with no additional regulatory costs. Industry will also be afforded the flexibility to address all hazard security threats in a manner they see fit.

### 4.2.3 Likely net benefit of option 1

It is anticipated that arguments put forward throughout this IA will demonstrate that option 1 is not capable of addressing the gaps which exist in Australia's transport sector. While, under the status quo, industry will face no increase in regulatory costs, stakeholders will suffer the forgone benefit of consistent and clear regulation and agile industry-led responses in the aftermath of an incident. Without addressing these gaps, the transport sector is left more vulnerable to a growing threat of all hazard incidents and the Australian economy is more exposed to the potential costs. The examples of potential all hazard incidents identified in section 1.1.2 and the potential costs of these incidents noted above, demonstrates the significant flow-on costs which can come from the disruption to the supply of goods, compromise of business operations, and other impacts. Consequently, over time the costs of option 1 are expected to far exceed the benefit of operation in a familiar, consistent regulatory environment.

### 4.3 Likely net benefit assessment: option 2

The following section details the costs and benefits associated with option 2 before assessing the overall likely net benefit presented by this option.

#### 4.3.1 Costs of option 2

Industry participants who choose to consider the guidance and information distributed through various engagement forums, and implement recommended activities to address all hazards threats, will incur costs anywhere between option 1 (status quo) and option 4 (regulation). The incurred costs will depend on the degree to which entities choose to enhance their practices in line with their improved understanding of the requirements and the changing threat environment.

For industry participants who choose not to consider the guidance and recommendations and information distributed through various engagement forums and do not implement recommended activities to address all hazards threats, the costs incurred will be the same as those costs associated with option 1. This is because such entities would continue to operate under the status quo regulatory environment with an unchanged exposure to the risks identified in question 1 of this IA. Given these risks are growing, there are potential additional costs associated with the realisation of, for example, a cyber-incident for an aviation or maritime entity.

For industry participants that do choose to voluntarily implement an all hazards security approach, the costs of this activity will be closer to that incurred under option 4 (refer to section 4.5.1 below for a description of these costs and the basis for the estimate included in this IA). Consequently, the overall cost of option 2 will be dependent on the proportion of entities which take-up an all hazards security approach and the extent to which entities fully or only partially implement the requirements of all hazards security. For the purposes of this analysis, it is assumed that the cost of option 2 could be between 20% and 40% of the cost of option 4. This would result in a one-off cost to industry of between \$38 million and \$135 million and an on-going cost of between \$23 million and \$81 million per annum. Given the voluntary nature of this option, it reasonable to assume that the total cost of this option is more likely to be at the lower end of this range.

Where the gaps identified in the existing framework regulating Australia's transport sector are not voluntarily addressed, industry and the Australian economy (including individuals, communities, and the environment) may incur additional costs, dependent on the severity and frequency of the disruption. As described previously in this IA, the current regulatory environment means government has limited visibility over industry's existing risk management practices. This limited ability to ensure risks are appropriately managed, compounds the potential additional costs for those entities who continue with the status quo, and enlivens a reputational risk for government where future incidents can be linked to gaps in the regulatory regime (as is the case in option 1).

Furthermore, Option 2 does not address the international standards or best practice relating to cyber security within the transport sector. For example, it would not consider:

- ICAO's Cybersecurity Policy Guidance, or Standard 4.9.1 of Annex 17, requiring cyber security be a regulated component of aviation security
- the IMO's Guidelines on Maritime Cyber Risk Management and the adoption of Resolution MSC.428(98) at its 98th session, which encourages governments to ensure cyber risks are appropriately addressed in existing safety management systems

#### 4.3.2 Benefits of option 2

Under option 2, industry will experience some of the benefits depending on the extent that industry participants voluntarily choose to address all hazard threats and consider mitigation strategies for the risks facing their business operations. The realisation of benefits is, however, inherently limited because participation is voluntary under option 2. Therefore, compliance with enhanced risk management standards and practices cannot be assured or enforced. Sector-wide compliance is crucial for supporting coordinated increase in risk management standards, strengthening industry resilience, and consistency in responding in the aftermath of an incident.

As such, only some benefits may be realised where industry chooses to engage with the voluntary requirements, including:

- enhanced understanding of the nature of growing security threats which are facing Australia's transport sector and an improved understanding of how risk management practice may be added to or changed to prevent and respond to such risks
- knowledge of the mechanisms available to support with incident planning, post-incident responses, and information sharing across entities through the forums described above (such as ASAF, RASAF, ACSIAF, MISCF, SASM and TISN)
- ongoing discussions between government and industry surrounding the need for enhanced risk management practices.

The voluntary approach may also offer industry some flexibility in choosing an approach to risk management which reflects the different risk appetites of industry participants' and government.

### 4.3.3 Likely net benefit of option 2

The costs and benefits set out above demonstrate that industry participants who choose not to consider the guidance and information distributed through various engagement forums will not contribute to achieving a coordinated increase in all hazards security risk management across Australia's transport sector.

Due to the size of the sector and large number of industry participants, it is difficult to estimate industry's engagement with the requirements of this option, however, considering the costs and benefits described above, the likely net benefit of option 2 would be higher than pursuing option 1, but lower than the likely net benefit offered by options 3 and 4. This is because the voluntary approach of option 2 means that it is unlikely to comprehensively address the problem areas outlined in this IA. Despite the benefits received by those industry participants who choose to voluntarily enhance their risk management practices, it is unlikely that a sector-wide increase will be achieved. Consequently, option 2 leaves Australia's transport sector vulnerable to the consequences of all hazard security threats, and will presents less economy-wide benefits as the likelihood and severity of all hazard incidents will remain without consistent sector-wide uplift in risk management practices.

## 4.4 Likely net benefit assessment: option 3

The following section details the cost and benefits associated with option 3, followed by an assessment of the likely net benefit presented by this option.

### 4.4.1 Costs of option 3

In 2021-22, consultation was conducted on the introduction of CIRMP obligations across several critical infrastructure sectors. This consultation exercise identified a range of costs arising for industry to comply with the CIRMP. Compliance with a CIRMP involves identifying and mitigating all hazards security risks. A summary of this data has been included below.

*Table 12: Regulatory cost per entity from 2021-22 consultation, indexed based on CPI to June 2024.*

	One-off Costs (\$ million)	Ongoing Costs (\$ million)
Critical infrastructure asset	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	9.2	4.3
Critical gas assets	12.0	2.4
Critical water assets	16.1	7.0
Critical data processing or storage assets	1.9	2.2
Critical broadcasting and domain name system assets	0.8	0.6

	One-off Costs (\$ million)	Ongoing Costs (\$ million)
Critical infrastructure asset	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical financial market infrastructure assets (payment systems)	0.1	1.6
Critical liquid fuels assets	10.1	3.0
Critical hospitals	14.8	11.5
Critical energy market operator assets	25.2	7.6
Critical freight infrastructure <i>and</i> critical freight services assets	4.4	2.6
Critical food and grocery assets	3.5	1.9
<b>Total average cost per entity</b>	<b>9.0</b>	<b>4.1</b>

These average costs per entity were the basis of a total range for expected compliance with the CIRMP rules, outlined in the table below. While the average costs per entity do not directly consider the potential costs of compliance for Australia’s transport sector, it is expected that costs would fall within the range indicated in table 12 above.

*Table 13: Summary of costs from 2021-22 consultation period, indexed based on CPI to June 2024.*

	Industry Costs (\$ million)	Community Costs (\$ million)	Individuals Costs (\$ million)	Total Costs (\$ million)
Cost type	Industry	Community	Individuals	Total cost
One-off	\$1824	Nil	Nil	\$1824
Ongoing (per year)	\$1226	Nil	Nil	\$1226

Beyond the quantified costs described above, additional costs associated with option 3 include:

- it would not capture all industry participants (for example tier 1 and 2 airports, and ship operators), as certain entities are not captured under the SOCI Act. The diversified nature of the transport sector would not be accounted for, as certain entities would not be required to mitigate risks such as cyber-attacks, supply chain risks and natural hazards. This would create security resilience gaps and inconsistency in security requirements across the sector
- it would not provide the government with adequate powers to enforce industry compliance with all hazard security obligations or to improve the security and resilience for the whole transport sector



- presenting an additional impost on industry, which would have to respond to security obligations across different legislative frameworks. Industry participants would be required to simultaneously maintain a security program (under ATSA or MTOFSA) and a CIRMP (under the SOCI Act), which would be both onerous and duplicative. These additional costs may be passed onto consumers through increased prices for goods and services.

Option 3 does not completely address the Cybersecurity Policy Guidance administered by ICAO, or Standard 4.9.1 of Annex 17, requiring cyber security be a regulated feature of aviation security. Although certain aviation assets will be required to mitigate cyber security risks, the guidance notes 'cybersecurity culture should be implemented across *all aviation entities*,' which is not upheld. The IMO's Guidelines on Maritime Cyber Risk Management and the adoption of Resolution MSC.428(98) at its 98th session is not adhered to by government under this option either, as it does not capture ship agents, port facilities, and all other maritime industry participants.

#### 4.4.2 Benefits of option 3

Reliable aviation and maritime services are central to Australia's prosperity. Disruption to the supply of essential goods and services, compromise of business operations, or other impacts on the transport sector can have a significant cost to the economy. There may be some benefit arising from option 3, where application of the SOCI Act can contribute to the avoidance of incidents that may otherwise disrupt operation and lead to economic loss. However, this benefit will only extend to those industry participants captured under the SOCI Act, rather than creating a potential benefit for the whole of Australia's transport sector.

This IA uses CGE modelling to demonstrate how costly a disruption to Australia's transport sector may be by examining a hypothetical 'shock' and an associated increase in input costs (i.e., an increase in the cost of the service). The advantage of using a CGE approach is both the direct and indirect (i.e. flow-on) economic impacts of an event can be quantified. This modelling will provide a baseline for comparing potential benefits across each option, but in particular options 3 and 4.

#### 4.4.3 Likely net benefit of option 3

In considering the costs and benefits described above, the likely net benefit of option 3 is higher than pursuing options 1 and 2, but lower than the likely net benefit offered by option 4. While the CIRMP framework will allow for consistent increase in the risk management practices amongst certain transport sector entities, it is not representative of the diversified nature of the sector. This option would result in a cohort of industry participants (such as tier 2 airports or ship operators) that are not required to identify and mitigate all hazards threats. Further, option 3 would not provide government with the full scale of power to support and enforce industry-wide compliance.

Where the bespoke threats facing Australia's transport sector are not addressed, the sector remains vulnerable to the consequences of all hazard threats. While the costs of option 3 are greater than compared to options 1 and 2, this is balanced by the threat of an incident and its impacts being lesser under option 3 because the uplift in risk management practices would be greater and more consistently applied. Option 3 also presents less economy-wide benefit when compared with option 4 (see analysis in question 7).

## 4.5 Likely net benefit assessment: option 4

The following section details the costs and benefits associated with option 4, followed by assessment of the overall likely net benefit presented by this option. The analysis will look at the proposed 15 measures captured under option 4 and consider the potential impacts to industry.

The costing and subsequent benefit analysis process for the aviation and maritime sectors has been undertaken at a consolidated level. This is due to the small number of cost impact responses received as part of consultation.

### Approach to determining likely net benefit: Breakeven analysis

A breakeven analysis was used to determine the net benefit of option 4. The breakeven analysis examined the number of incidents that must be avoided (i.e. the benefit) each year for the annual costs of the option to be met.

While this IA sought to leverage real life examples of the potential disruptions caused by the realisation of all-hazard security events, this does not mean that equivalent events must occur for the costs and benefits outlined in this IA to break even. For example, while the IA used the British Airways data breach as a 'moderate' scenario, an accumulation of many, smaller disruptions would also deliver the same benefits against the proposed reforms, as discussed in section 4.5.2 below.

The rationale for use of breakeven analysis is that the total benefits of the option 4 consist of the avoided or mitigated costs of future all-hazard security incidents. However, the total annual benefit cannot be reliably estimated because there is no data on the frequency and size of avoided incidents. Any estimate of total benefits would be highly uncertain, contestable and reliant on assumptions.

The use of a breakeven analysis avoids the need for this information, and instead uses an assessment of the reasonableness of the number of avoided incidents required for option 4 to equal or exceed the costs of the option. The breakeven analysis was calculated by determining the number of severe, moderate, and low scenarios needed to be avoided each year to equal the annual cost of the regulation.

The following formula was used to determine the breakeven point:

$$\text{Number of severe/moderate/low scenarios required to be avoided per year for net benefit to occur} = (\text{total cost to the economy of severe/moderate/low scenario}) / (\text{annualised cost of regulation})$$

#### 4.5.1 Costs of option 4

Table 14 describes the cost impact of each of the 15 measures and provides a summary of responses from industry about the potential impact. Table 21 identified how the policy positions outlined below were informed by industry consultation, contributing to a more applicable reform option for industry that results in a smaller anticipated cost.

Table 14: Indicative costs of measures

Measure	Department's estimated impact	Industry Responses
<b>Resilient to current and emerging threats</b>		
<p><b>Measure 1:</b> Expand the definition of unlawful interference to capture a variety of acts, including cyber security incidents, and expand security incident reporting requirements</p>	<p>Minimal cost impacts are expected with this legislation change; it is assumed that increasing the scope of enforcing existing regulations will have a minimal impact to industry.</p> <p>Consultation on the Independent Review resulted in a department decision to no longer proceed with the requirement to report cyber-related attempted acts of unlawful interference. This will limit the cost impact of this measure. Further information on the consultation process is provided in Section 5.</p>	<p>Submissions from industry noted that there will be some cost implications as a result of this change. Where responses from industry quantified these costs, they have been considered together with costs for measure 2 and are shown in table 15 below.</p>
<p><b>Measure 2:</b> Introduce all hazard security obligations requiring that captured industry participants identify and mitigate cyber, supply chain and natural hazard risks (in addition to physical and personnel security risks) under a single legislative framework</p> <p>Obligations will apply differently across industry and hazard domains. For a proposed structure of all hazard obligations by cohort, see Appendix B</p>	<p><b>Risk assessment:</b> Some costs expected to arise due to increase in capability requirements. Cost impact is dependent on the complexity of the business affected.</p> <p><b>Physical:</b> Nil to minor costs expected given existing obligations</p> <p><b>Personnel:</b> Minor costs expected given existing obligations (see measure 3 below)</p> <p><b>Cyber:</b> Minor to moderate costs expected due to increase in capability requirements. Costs would be dependent on whether a staged approach is applied and level of maturity of the business affected.</p> <p><b>Supply chain:</b> Some costs expected to arise given no existing obligations. Cost impact is dependent on the complexity of the business affected.</p> <p><b>Natural hazard:</b> Some costs expected to arise given no existing obligations. Cost impact is dependent on the complexity of the business affected.</p>	<p>Industry agreed that there will be cost implications as a result of this change. These costs have been considered in table 15 below.</p>

<p><b>Measure 3:</b> Introduce a requirement for industry to identify and mitigate risks associated with personnel who have access to, of influence of, secure areas, or critical systems, remotely</p>	<p>Some costs expected to arise given potential cost of implementing some mitigation measures</p>	<p>Submissions from industry indicated there may be a minor cost impact on industry as a result of requirements to introduce additional mitigation activities, arising from changes in definitions under measure 3. These cost impacts were included in estimates for measure 2 for those industry submissions which quantified the impact. Consequently, the cost impact of the measure is included in the costs presented in table 15 below</p>
<p><b>Effective system testing program</b></p>		
<p><b>Measure 4:</b> Amend the definition of test weapons to align with likely threat scenarios</p>	<p>Due to the change only expanding the criteria of test weapons in the transport security legislative frameworks, it is expected to have only a minor impact to industry. Processes for managing test weapons should already exist and so the marginal impact of the definitional change will be minor</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>
<p><b>Measure 5:</b> Introduce vulnerability testing on Australian aviation and maritime security systems</p>	<p>Potential impacts arising from any additional effort or time required to prepare for vulnerability testing on aviation security systems</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>
<p><b>Measure 6:</b> Introduce maritime system and vulnerability testing and provide MSIs with equivalent protection and powers that ASIs currently possess</p>	<p>It is expected there will be a nil impact to industry participants as a result of this change</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>

Robust compliance and enforcement framework		
<b>Measure 7:</b> Align SSD powers to be given where there is specific, or changed general threat or risk across all hazards	Potential impacts depend on the nature of the direction, including time and costs associated with responding to the direction. These impacts are limited by the fact that an SSD power already exists. This cost will create no cost impact for industry	Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry
<b>Measure 8:</b> Extend the demerit points system to the air cargo sector. Compliance activities are already conducted against the air cargo sector, and this reform will allow for an accumulation of non-compliance to result in cancellation or revocation of their security program	It is expected that where there is no change to existing compliance activities and no new industry participants are captured by compliance requirements, there will be nil cost impact to industry	Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry
Modernisation and proportionate regulation		
<b>Measure 9:</b> Allow training requirements for cargo-examining aircraft operators to be made through determinations to align with the rest of the air cargo sector	It is expected the change will have a nil impact to industry participants, as there will be no change to training requirements, only how they are prescribed	Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry
<b>Measure 10:</b> Align the powers for authorising a charging fee for issuing a security identification card across the transport security legislative frameworks	Minimal cost impacts to industry due to this change noting that some costs (e.g. associated with producing an aviation security identification card, hereto referred to as an ASIC) are already recovered	Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry
<b>Measure 11:</b> Ensure maritime entities that impact critical functions are subject to security obligations	It is expected some costs will arise as a result of the change, as the measure may create new obligations for some industry participants	Submissions from industry indicated either agreement or did not disagree that there will be a minor impact to industry following reassessment of critical functions

<p><b>Measure 12:</b> Remove the requirement for ships that operate as both a ship and offshore facility to have two security plans</p>	<p>It is expected this change would not result in a cost burden to industry, but rather provide a small cost savings to industry and the department due to the reduced number of security plans needed for each vessel and voyage</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>
<p><b>Measure 13:</b> Remove the requirement for a security plan for ships that infrequently travel internationally</p>	<p>It is expected this change would not result in a cost burden to industry, but rather provide a small cost savings to industry and the department due to the reduced number of security plans needed for each vessel and voyage</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>
<p><b>Measure 14:</b> Replace 'sex' with 'gender, if practicable'</p>	<p>It is expected there will be a nil impact to industry participants as a result of this change</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>
<p><b>Measure 15:</b> Remove references to 'fax'</p>	<p>It is expected that expanding the available technology would allow for better communication and a minor reduction in business costs</p>	<p>Submissions from industry indicated either agreement or did not disagree that there will be nil cost impact to industry</p>

Cost submissions in relation to measures 1 and 2 were received from 3 industry participants from the aviation sector. These responses were from entities representing approximately 40% of the total aviation transport market. Cost submissions were received from 1 industry participant for the maritime sector. This response was from an entity representing approximately 9% of the total maritime market. An indicative costing of measures 1 and 2 is provided below.

There are multiple factors affecting the cost impact for each entity, including their existing risk management practices and capabilities, the nature of the critical assets they operate and the size of their operations. In collecting cost information from entities across the aviation and maritime sectors, this variance in cost impact has been captured and reflected in the estimates of total cost across the asset classes included in this IA.

When estimating the cost of compliance with option 4, an expected and a high-cost estimate has been included. The high-cost estimate was provided as a way to measure the uncertainty associated with an entities estimate and the highest feasible cost of option 4. The expected estimate was used as the basis for determining the net benefit of option 4 in section 4.

Using the expected and high estimates as a range, the direct cost of compliance is as follows:

- A one-off (establishment) regulatory cost between \$190 million (expected) and \$336 million (high estimate), across the aviation and maritime sectors.
- An ongoing cost between \$115 million (expected) and \$203 million (high estimate) per year, across the aviation and maritime sectors.

The cost of regulation will be borne by entities responsible for aviation and maritime sectors who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this IA, the cost of regulation in the table below will only include the direct costs associated with regulation. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy because of the proposed legislative amendments.

*Table 15: Regulatory cost estimate (expected)*

Sector	Cost type	Industry Costs (\$ million)	Community Costs (\$ million)	Individuals Costs (\$ million)	Total Costs (\$ million)
		Industry	Community	Individuals	Total cost
Aviation	One-off	61	Nil	Nil	61
	Ongoing (per year)	59	Nil	Nil	59
Maritime	One-off	129	Nil	Nil	129
	Ongoing (per year)	56	Nil	Nil	56
Total Transport	One-off	190	Nil	Nil	190
	Ongoing	115	Nil	Nil	115

Based on the industry submissions made during consultations, costs of this reform will be highest for obligations associated with measure 2 and most notably, personnel, supply chain, cyber security, and natural hazards (noting obligations will apply differently across industry participants and hazard domains – see Appendix B for a proposed structure of all hazard obligations by entity). These costs represent approximately 82% of the total cost of implementing this reform. This emphasis on measure 2 costs (and personnel, supply chain, cyber security, and natural hazards in particular) is because some aspects of the reforms are already captured under the existing transport security legislative frameworks (including special security directions, and screening requirements). Industry already incur the compliance costs of these existing obligations and so no additional uplift in capability (or cost) will be required to address these new requirements.

The cost estimates provided will be smaller in practice once considering that numerous mature industry participants are already operating at a level that would make them compliant with the proposed obligations for measure 2. This includes a cohort of entities that will be subject to cyber security and supply chain obligations.

*Table 16: Regulatory cost estimate (expected) cost by measure*

Sector Costs by measure	One-off	Ongoing (per year)
Measure 1 - Unlawful Interference		
Expand Definition of Unlawful Interference and reporting requirements	5%	8%
Measure 2 - All hazards security framework		
Personnel Security*	33%	28%
Cyber Security	16%	25%
Supply Chain	20%	17%
Natural Hazards	13%	10%
All Hazards Risk Assessment & Attestation	14%	11%
<b>Total cost (\$ million)</b>	<b>190</b>	<b>115</b>



\*Note: The costs of personnel security obligations would vary based on the size and complexity of the entity affected. Industry submissions which provided an estimate of the costs of compliance with proposed personnel security obligations suggested a correlation between the cost of the personnel security function and the size of the entity (measured in full time equivalents). Smaller entities reported lower anticipated compliance costs than larger entities with complex, remote roles which can affect the function of secure zones. Submissions also suggested that entities with no requirement to perform security functions or to control access to security zones remotely would not incur any additional costs from the security controlled activity measure.

The information presented in tables 15 and 16 is disaggregated to the greatest extent possible while not identifying the entities who submitted information to the department.

#### 4.5.2 Benefits of option 4

Disruption to supply, compromise of operation, or other impacts on the transport sector can have a significant cost to the economy. Bespoke reforms can address the frequency and impact of any disruption to the availability, integrity, reliability, or confidentiality of Australia's transport sector. There is also a direct link between implementation of option 4 and the achievement of key objectives including ensuring government and industry are equipped to respond to current and emerging threats; ensuring industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards threats; and ensuring Australia is proactive and adaptive to evolving international obligations, to remain compliant and stay informed of global standards and developments relating to aviation and maritime security. Together, these objectives will ensure desired security outcomes are met.

Other benefits associated with option 4 may include:

- increased protection for the transport sector from all hazards security risks that may disrupt operations
- reduced likelihood and severity of all hazards events, such as cyber-attacks
- assistance for industry, including government intervention where appropriate, to mitigate the consequences of these incidents on Australia's transport sector
- support from government to seamlessly coordinate cyber security incident responses
- flexibility in responding to evolving threats and the potentially significant impact of an all hazards event on the Australian economy and community
- proactively addressing and mitigating any risks which an entity may become aware of when conducting risk management activities
- complete adherence to the requirements of ICAO and the IMO.

#### Economic impacts of disruptions to aviation and maritime sectors

Disruptions that affect the transport sector can subsequently disrupt the flow of goods across the economy, which can affect business and households. Even small disruptions to major transport control systems can quickly cascade into significant sector and nation-wide economic disruptions. These events can generate costly immediate and longer-term impacts on the Australian economy. Immediate impacts of an aviation or maritime disruption are those associated with the transport of goods across the supply chain and can cause upstream and downstream impacts, such as:

- loss of productivity as a result of disrupted economic activity (e.g. workers may be idle whilst continuing to receive wages)
- lost wages (e.g. workers may be sent home or unable to go to work)
- delays in public aviation transport (e.g. hotel costs, meal vouchers, rescheduling costs)
- spoiled goods (e.g. goods that may have a short shelf life, such as produce)

- additional holding costs (e.g. storing refrigerated goods for longer periods of time)
- disruptions to transport services can result in supply shortages for the food and grocery sector, and in available medicines
- other critical infrastructure sectors such as the energy sector and data storage or processing rely of transport services to remain operatable, risking widespread outages or inoperability of essential services.

### Computable General Equilibrium (CGE) modelling approach

A scenario based on a disruption to a maritime sector entity was selected due to the availability of information and quantitative evidence. To analyse the direct and indirect economic contributions of the disruption, a CGE approach was used to model the economy as a system of interrelated economic agents operating in competitive markets. Economic theory is used to specify the behaviour and market interactions of economic agents, including consumers, investors, producers and governments operating in domestic and foreign goods, capital and labour markets.

Defining features of the theoretical structure of the model are:

- optimising behaviour by households and businesses in the context of competitive markets with explicit resource and budget constraints
- the price mechanism operates to clear markets for goods and factors such as labour and capital (i.e. prices adjust so that supply equals demand)
- at the margin, costs are equal to revenues in all economic activities.

The modelling framework is suited to analysing the economic impact of an aviation or maritime disruption as it explicitly captures supply chain linkages as well as other flow-on effects and feedback responses by all economic agents. The strength of CGE models is that they capture the upstream and downstream linkages between the activities induced by the outage and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

### Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the aviation and maritime system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the impact of a disruption to the aviation and maritime sectors. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

## Case Studies

The case studies provided in the table below provide a basis for modelling hypothetical but comparable incidents in an economy-wide model and contextualises the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe incidents.

*Table 17: Aviation and maritime case studies*

Incident	Summary of incident
DP World cyber-attack (2023)	On 10 November 2023 Australia's second largest port facility operator, DP World, which is responsible for 40% of maritime freight in Australia, was shut down due to a cyber security incident which impacted the movement of goods in and out of Australia. <sup>46</sup> Ships remained able to unload freight to the port, however, freight could not leave the port. DP World contained the incident, recommencing operations on 13 November 2023 and by 20 November 2023 was able to clear the backlog comprising of approximately 30,000 containers. <sup>47</sup>
British Airways data breach (2018)	In 2018, British Airways fell victim to a cyber-attack when malicious actors hacked the company's website and app and stole data from approximately 430,000 customers (with 58% of these customers experiencing theft of their crucial details including credit card details and CVV codes). In the aftermath of the attack, Britain's Information Commissioner's Office in October 2021 fined British Airways 20 million pounds (AUD38.7 million). A class action followed the incident, with a group of 23,000 (as at July 2021) claimants suggesting they incurred damages as a result of the hack. <sup>48</sup> Based on publically available data, the total cost of the data breach to the airline was as much as AUD129 million in fines and compensation. This does not include any additional costs associated with strengthening cyber security (about which the airline made no public announcement).
Port of Brisbane, impact of Brisbane floods (2011)	On 12 January 2011, the Port of Brisbane was closed to ships for 10 days due to elevated water levels, underwater debris and strong under currents as a result of flooding, preventing the safe movement of vessels. The closure caused an estimated impact of \$50 million in losses, reducing the Port's annual throughput by 6.4 per cent. <sup>49</sup>
Port of Baltimore, impact of collision between cargo ship and key bridge (2024)	On 26 March 2024, a cargo ship crashed into Baltimore's Key bridge, severing access to critical shipping routes in and out of the Port of Baltimore. The Port was closed for 71 days, with the daily economic impact estimated to be approximately USD15 million (AUD22.8 million), representing an AUD1.6 billion economic impact as a result of the incident. <sup>50</sup>

<sup>46</sup> Major Australian port operator shuts down, ABC News, 2023, [abc.net.au/major-australian-port-operator-shuts-down](https://abc.net.au/major-australian-port-operator-shuts-down)

<sup>47</sup> Media Statement, DP World, 2023, [dpworld.com/media-statement-update-on-cyber-incident](https://dpworld.com/media-statement-update-on-cyber-incident)

<sup>48</sup> British Airways class action settlement, Herbert Smith Freehills, 2021, [www.herbertsmithfreehills.com/british-airways-class-action-settles](https://www.herbertsmithfreehills.com/british-airways-class-action-settles)

<sup>49</sup> Climate change and adaptation planning for ports, Taylor & Francis Group, 2015, [taylorfrancis.com/climate-change-and-adaptation-planning-for-ports](https://taylorfrancis.com/climate-change-and-adaptation-planning-for-ports)

<sup>50</sup> Shipping closure at Port of Baltimore could have economy wide impacts, WYPR, 2024, [wypr.org/shipping-closure-at-port-of-baltimore](https://wypr.org/shipping-closure-at-port-of-baltimore)

These case studies highlight that disruptions to the aviation and maritime sectors can inflict significant direct and indirect costs to entities and individuals alike. For the purposes of the modelling of the cost of avoided future incidents, consideration has been given to a range of cost impacts based on real world events. The British Airways data breach in 2018 was used as the baseline (moderate) scenario in the break-even analysis presented below (and shown in table 18 below). The use of an actual event as a point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling. It is estimated the impact of the data breach to be \$129.0 million of direct costs to British Airways, with additional indirect costs likely affecting the broader economy.

Based on this approach, a framework for considering the potential impacts of the aviation and maritime incidents is provided in the table below.

*Table 18: Framework for scenario development and sensitivity analysis*

	<b>Severe scenario</b>	<b>Moderate scenario</b>	<b>Low scenario</b>
Intensity of event	Port closure of 22.2 days noted in the 'Port disruptions due to natural disasters' study (2020)	British Airways data breach (2018)	50% of Moderate scenario costs

The rationale for considering less severe scenarios than experienced in the British Airways data breach reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month, day of the week, or the time of day at which the disruption occurs and the duration of the disruption. It is necessary to account for an incident that has a greater and a lesser economic impact than the British Airways data breach to reflect the possibility that a disruption of a similar scale could impact areas where there would be different economic impact. While an incident with a much greater impact than the severe scenario is conceivable,<sup>51</sup> the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

In this context, the severe scenario in table 18 assumes a port closure of 22.2 days consistent with the 95% percentile reported in the port resiliency study referenced above. The daily cost of the Port of Baltimore incident (AUD 22.8 million) was applied to this assumed port closure of 22.2 days to provide an estimated total cost of \$506.2 million. The low scenario in table 18 accounts for incidents that have a lesser economic impact than the moderate scenario (assumed to be 50% of the moderate scenario).

<sup>51</sup> Demonstrated by the larger impact of the Port of Baltimore incident described in Table 15.

A summary of the economic impact of each scenario is provided in table 19 below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the all hazards security framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of option 4 to equal the costs of implementation and compliance.

*Table 19: Summary of benefits for each scenario*

	Scenario 1 (Severe)	Scenario 2 (Moderate)	Scenario 3 (Low)
Direct avoided cost (\$ million)	\$291.5 million	\$129.0 million	N/A
Indirect avoided cost (\$ million)	\$214.7 million	Nil *	N/A
Total avoided cost to the economy of the incident (\$ million)	\$506.2 million	\$129.0 million	\$64.5 million <sup>52</sup>
Approximate number of avoided incidents per annum required for a net benefit	1.3	5.3	10.6

\*Note: The nature of the incident costs (a fine and compensation as part of a class action) are such that they primarily impact the entity. While entities typically pass on enforcement and compensation costs to customers (indicating some economy-wide indirect costs), given the incident's estimated direct costs include some uncertainty, a conservative approach to the break-even analysis has been applied and no indirect costs have been assumed in relation to this Moderate scenario. While it is reasonable to assume that British Airways incurred additional costs associated with strengthening cyber security, there is no publicly available information which quantifies this cost and so these costs have not been considered as part of the break-even analysis. If these costs were incurred, it would lower the number of break-even avoided incidents.

As noted above, the total direct ongoing cost for option 4 is expected to be \$115 million per annum plus direct one-off costs of \$190 million. However, the cost of the all hazards security framework may also have other indirect costs flowing from increased prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change per year costs would be approximately \$681.9 million. This considers the cost of providing aviation and maritime services, and the total economic cost of the regulatory changes including direct and indirect impacts. In order for the regulatory changes to generate a net benefit, the proposed all hazards security framework would need to contribute to the prevention of approximately 1.3 severe scenarios per year, 5.3 moderate scenarios per year or 10.6 low scenarios incidents per year.

<sup>52</sup> Cost of \$64.5 million being 50% of the cost of the moderate scenario.

It is important to note the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the case studies considered. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances, which were not experienced during the 3 case studies considered above. Consequently, the severe case of a port closure of 22.2 days (noted in the 2020 study), may not be the worst-case incident and an incident of the same scale could have a greater impact if it occurred in other locations (for example, larger ports with higher value trade) or at other times (for example, in the lead-up to Christmas when delays to imports may incur greater costs to retailers). The Port of Baltimore case study also demonstrates that a port closure in excess of 22.2 days is plausible.

In the aviation and maritime sectors, the economic benefit of avoiding incidents should also be considered alongside the avoided cost to human life. These impacts have not been modelled because they were not a consequence of the 2 case studies examined. The estimated value of a statistical life (the value society places on reducing the risk of dying) is \$5.4 million, and the value of a statistical life year (the value society places on a year of life) is \$0.235 million.<sup>53</sup> As both aviation and, to a lesser extent, maritime services are critical to human life (including transport of passengers and delivery of various essential goods), any avoidance of an incident that could otherwise increase the likelihood of risks to human life will have a benefit beyond that of the avoided cost to the economy able to be modelled.

Further, the increasing frequency and severity of incidents as described in section 1.1 makes the benefits of the proposed all hazards security framework more certain over time to exceed the anticipated costs. The examples referred to in that section include increasing cyber incidents in relation to critical infrastructure in general and aviation and maritime industry participants in particular. In addition, it is reported that natural disasters fuelled by the climate crisis will continue to intensify. These hazards have and will cause, widespread and substantial impacts, losses and damages, including potential damage to infrastructure, coastal areas (including low lying port infrastructure). The growing frequency and severity of incidents demonstrate the increasing need for adequate protections against the security and resilience of aviation and maritime critical assets. This also indicates the benefits of the all hazards security framework will further exceed the costs over time.

---

<sup>53</sup> Value of Statistical Life, PM&C, 2023, [oia.pmc.gov.au/value-of-statistical-life](https://oia.pmc.gov.au/value-of-statistical-life)

### 4.5.3 Likely net benefit of option 4

The likely benefits of option 4 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout the IA, the frequency and severity of all hazard risks for the aviation and maritime sectors are growing. While some events of the magnitude described in the IA have previously been considered to represent the worst-case disruption scenarios in Australia, the increasing severity and frequency of similar incidents, particularly in the context of growing cyber security incidents represents a risk to the whole economy. The increasing frequency of incidents as described above, makes the proposed all hazards security framework more likely to exceed the anticipated costs over time.

Further, through the pursuit of option 4, the identification, mitigation and remediation of such hazards should they occur, will be improved through:

- lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for aviation and maritime industry participants
- ensuring that adoption of the all hazards security framework for aviation and maritime industry participants is reasonable and proportionate to the purpose of the program
- ensuring the transport security legislative frameworks are robust, proportionate, and fit-for-purpose to meet security objectives.

Overall, these factors and the specific costs and benefits described above mean that the likely net benefit associated with option 4 is high.



# 5. Who did you consult and how did you incorporate their feedback?

This section provides an overview of consultation undertaken by the department on the potential reform measures considered in this IA. It summarises the purposes and objectives of consultation, a summary of the approach to consultation, as well as analysis of outcomes and key themes.

## Purpose and objectives of consultation

Continuous and broad-based consultation is an essential component of the department's process for understanding industry's views on aviation and maritime security legislation and reforms. Consultation is essential for ensuring that all enacted reforms are implemented in a manner that achieves desired outcomes, while minimising any unnecessary or disproportionate costs on Australia's transport sector.

The department's commitment to consultation also reflects the view that each sector manages risk in a unique way and that industry stakeholders themselves are best placed to identify, evaluate, and mitigate the risks that manifest in their particular operating environment. The department acknowledges and seeks to avoid broadly applicable, prescriptive legislative reforms, which have the potential to disrupt industry's ability to respond to risks in a nuanced manner. Effective consultation is critical for the department in validating the nature of the proposed reform measures, allowing organisations to continue managing their risks in a manner most appropriate for their operating context.

## 5.2 Summary of consultation completed

The department has completed a period of targeted consultation with industry on the 15 proposed reform measures contained within a consultation paper and considered in this IA. This engagement occurred across February, May, July and October 2024, and has included:

- **Targeted industry consultation on the Security Controlled Activities measure.** This consultation sought to understand at a high-level, which specific work-related activities should be captured. The department distributed a discussion paper, held a roundtable, held three bilateral meetings and attended a port. Submissions were provided in response to our consultation paper.
- **Establishment of the Transport Security Reform Advisory Committee (TSRAC),** to provide strategic advice to the department on the development, and implementation, of the measures. Member comprise industry co-chairs from ACSIAF, ASAF, RASAF, and MISCF, as well as representative industry bodies. TSRAC has met twice – to discuss the measures, and to discuss the outcomes of industry feedback.
- **Inviting industry to make a written submission in response to a Consultation Paper.** The paper described each proposed measure, its rationale and indicated how the measure may operate in

practice. The department also posed questions to industry on how it could support industry to meet the new legislative requirements, with a view to receiving input.

- **Consultation with industry through the early assessment IA**, assessed as adequate for consultation by the OIA, to support identification and evaluation of potential regulatory impacts. When distributing the IA, the department offered one-on-one sessions with industry participants to answer questions and support industry's estimation of regulatory impacts (in addition to the virtual consultation sessions outlined below). The department held 3 of these session upon request.
- **Virtual consultation sessions on the content of the Consultation Paper and IA**. This consultation, held via Microsoft Teams were designed to provide industry with opportunities to seek further information on the reforms. The consultation period ran for around four weeks and included:
  - two town hall meetings, with approximately 66 participants in attendance across both sessions
  - 6 sector-specific round tables (two for each of maritime, aviation and air cargo), with approximately 133 participants in attendance across all sessions
  - 3 sessions (one for each of maritime, aviation and air cargo) focused on assisting industry with completing a costing template which was distributed alongside the IA.
- **Bilateral meetings to discuss questions raised in written submissions** were also held on request and facilitated as high as at the Deputy Secretary level to discuss concerns and provide clarity about the proposed implementation of the reforms.
- **Measure specific town halls** on measures 3 (security controlled activities) and 11 (regulate the right entities) to allow industry to speak with the internal subject matter experts.
- **Consultation with industry to the first pass IA**. This consultation invited participants to provide written submissions in response to the first pass IA. Industry participants were asked to provide confirmation of the:
  - reasonableness of the net benefit conclusions for options 1,2,3 and 4
  - reasonableness of the assessment of cost impact summarised in table 16 (formerly 14)
  - split of costs between obligations in option 4 and presented in table 16 (formerly 14)
  - reasonableness of the 'best option' conclusion in section 6.

In addition, one town hall meeting was held with approximately 65 attendees. The department offered one-to-one follow-up sessions at the conclusion of the town hall. The department held one session upon request. The department received 10 submissions to the first pass IA.

- The development of the measures considered through these consultation forums was informed by earlier consultation on the Independent Review. A summary of industry responses to the

Independent Review is summarised in table 20 below. A summary of the department's changes made in response to industry's feedback is provided in table 21.

### **5.2.1 Feedback received through consultation on the Consultation Paper**

The Consultation Paper was released on Friday 27 May 2024, requesting written submissions be sent to the department by 28 June 2024 (noting the department agreed to extensions to this deadline for numerous IPs to encourage comprehensive submissions). The department sought submissions from just over 3000 stakeholders on the Consultation Paper and IA, with 23 entities providing written submissions to the Consultation Paper.

Consultation on the transport security reform package was supported by industry. The majority of the feedback provided comprised feedback on how the reform package could be refined, with entities expressing a keen desire to continue engaging with government to take the reform package forward.

The table below summarises industry views provided in response to the Consultation Paper and identifies the department's proposed response or actions arising as a result of industry feedback.

### **5.2.2 Consultation on the Independent Review of Australia's Aviation and Maritime Security Settings**

Consultation with industry occurred following the Independent Review. The Hon Clare O'Neil former Minister for Home Affairs and Minister for Cyber Security, invited more than 1,795 aviation and maritime industry participants, to provide submissions on the Independent Review Final Report and related discussion paper between 31 March and 12 May 2023.

The department received 38 industry submissions in response to the discussion paper, which are summarised in the table 20 below.

*Table 20: Summary of industry submissions to Independent Review*

Proposal	Summary of submissions received
<p><b>Proposal 1:</b> Reduce prescription of security programs</p>	<p>29 entities agreed, or agreed in principle. 3 entities did not agree. 6 entities noted or did not comment.</p> <p>Majority support for reduced prescription in security programs.</p> <p>Guidance and support from the Regulator should accompany any legislative reform to reduce prescription.</p>
<p><b>Proposal 2:</b> Move to an outcomes and risk-based security management approach</p>	<p>22 entities agreed, or agreed in principle. 3 entities did not agree. 10 entities noted or did not comment.</p> <p>General support for an outcomes-based framework that includes the introduction of a Security Management System, where voluntary and accompanied by guidance.</p>
<p><b>Proposal 3:</b> Enable department to intervene and take a more direct regulatory role with screening and other security providers</p>	<p>20 entities agreed, or agreed in principle. 6 entities did not agree. 12 entities noted or did not comment.</p> <p>Emphasis on ensuring transparency in any additional regulatory relationships with third parties.</p> <p>Concerns related to duplicative effort, inconsistent messaging and its impact on contractual relations between an entity and third party provider.</p>
<p><b>Proposal 4:</b> Requiring screening airports to screen for all regular public transport and open charter flights</p>	<p>12 entities agreed, or agreed in principle. 6 entities did not agree. 20 entities noted or did not comment.</p> <p>Requirement that all screening airports screen regular public transport and open charter flights generally supported by major airlines and airports.</p> <p>Concerns raised on the costs and personnel burden this may create for regional airports.</p>
<p><b>Proposal 5:</b> Opportunities to broaden and improve industry engagement, partnership and collaboration</p>	<p>29 entities agreed or agreed in principle. 0 entities did not agree. 9 entities noted or did not comment.</p> <p>Broad agreement of benefits that arise from increased collaboration between government and industry. Welcomed opportunities to enhance existing engagement initiatives and receive more guidance material from the department, to help industry in meeting security obligations and on the broader risk environment.</p>

Table 21: Responses to industry consultation

No.	Measure	Initial approach	Industry feedback	Updated approach following consultation	Additional considerations
	General		<ul style="list-style-type: none"> <li>Enquired how the reforms address the outcomes of the Independent Review</li> </ul>		<ul style="list-style-type: none"> <li>The reforms address the Independent Review holistically. The reforms are multi-faceted and comprise a legislative and regulatory reform package, and an uplift of government and industry capability and partnership</li> </ul>
1	Expand the definition of unlawful interference (UI)	<ul style="list-style-type: none"> <li>Expand the definition of UI to include a variety of acts, including cyber security incidents</li> <li>Introduce security incident reporting requirements for cyber security incidents and attempted acts of UI</li> <li>In MTOFSA, remove 'terrorist act' within the security incident definition to align the reporting requirements with the expanded definition of UI and the introduction of all hazards security obligations</li> </ul>	<ul style="list-style-type: none"> <li>General support to incorporate cyber security incidents within the definition of UI</li> <li>Further clarification sought on what will constitute an attempted act of UI and terms such as 'assets'</li> <li>Concerns raised included the short timeframes for reporting, the potential duplicative reporting burden, and the difficulty with identifying and reporting cyber-related attempted acts of UI</li> </ul>	<ul style="list-style-type: none"> <li>No longer proceeding with the requirement to report cyber-related attempted acts of UI, due to its ambiguity</li> </ul>	<ul style="list-style-type: none"> <li>There will be <u>no</u> dual reporting obligations for IPs. Cyber security incidents will <u>not</u> need to be reported by IPs under both the SOCI Act and the ATSA/MTOFSA</li> <li>The government is developing a single cyber incident reporting portal that will aim to reduce administrative burden when reporting incidents</li> <li>We will provide guidance on the new requirements, including on: <ul style="list-style-type: none"> <li>attempted acts of UI</li> <li>scope of cyber incident reporting, including for international incidents</li> <li>definitions such as an 'asset' and 'relevant impact'</li> </ul> </li> </ul>
2	All hazards security framework	<ul style="list-style-type: none"> <li>Introduce all hazard security obligations requiring industry participants to manage risks associated with physical and personnel threats, cyber incidents, supply chain disruptions and natural hazards</li> <li>Introduce/expand the requirement to submit an all hazards risk assessment, identifying risks relevant to the industry participant's threat and operating environment and appropriate mitigation measures, alongside an industry participant's security program</li> <li>Require yearly, at a minimum, an industry participant's board or governing body to attest the</li> </ul>	<ul style="list-style-type: none"> <li>General support. Note it would be resource intensive, may be duplicative to obligations under other legislative frameworks, and asked for comprehensive guidance to support implementation</li> <li>The requirement to provide an attestation more frequent than annually may be overly onerous</li> <li>More information sharing, including transport sector-specific risk and threat information, would be required to support the transition to the new all hazards security framework</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial approach</li> </ul>	<ul style="list-style-type: none"> <li>We are consulting internally on the best approach to sharing risk and threat information with industry</li> <li>We will provide guidance on the new requirements, including: <ul style="list-style-type: none"> <li>addressing duplicative obligations under other legislative frameworks</li> <li>on the risk assessment, including the scope of risks that may be considered, and where supporting documentation can be relied on</li> <li>the attestation</li> <li>the scope of the supply chain security obligations</li> <li>the assessment process for the new obligations, including if you hold a CIRMP under the SOCI Act</li> <li>on implementation</li> </ul> </li> </ul>

Table 21: Responses to industry consultation

No.	Measure	Initial approach	Industry feedback	Updated approach following consultation	Additional considerations
		mitigation measures address the identified risks, meet legislative requirements and is within the board or governing body's agreed risk tolerance			
3	SCA	<ul style="list-style-type: none"> <li>Identify SCAs through a risk assessment and implement appropriate mitigation measures to manage risks associated with personnel undertaking SCAs</li> <li>Mitigation measures for SCAs may include requiring relevant personnel to hold an aviation and maritime security identification card (ASICs/MSICs), or implementing processes or procedures to ensure the security of relevant areas, information and systems</li> <li>For international-based personnel or third party suppliers, an industry participant will be required to attest the personnel or entity it has engaged aligns with its legislative obligations and meets desired security outcomes</li> </ul>	<ul style="list-style-type: none"> <li>General support with guidance sought on how to define SCAs</li> <li>Lack of clarity on the voluntary/risk based nature of subjecting employees undertaking SCAs to ASIC/MSICs, with further guidance sought on alternative mitigation measures that could be implemented</li> <li>Concerns over increased costs and delays for obtaining ASICs/MSICs and the further pressure that may place on AusCheck as the single issuing body</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial approach</li> </ul>	<ul style="list-style-type: none"> <li>In February 2024, following targeted high-level consultation with industry participants, we changed the approach from prescribing SCAs, to requiring industry participants to self-identify SCAs through a risk assessment, and implementing appropriate mitigation measures to manage risks associated with personnel undertaking SCAs</li> <li>The CISC intends to engage closely with impacted industry stakeholders to anticipate and plan for increased volume demand and mitigate any potential delays to ASIC-MSIC background checking processing times for applicant cohorts</li> <li>We will provide guidance on the new requirements, including: <ul style="list-style-type: none"> <li>the types of activities that may be considered an SCA</li> <li>mitigation measure options</li> </ul> </li> </ul>
4	Amend the definition of 'test weapon'	<ul style="list-style-type: none"> <li>Amend the definition of test weapon to align with likely threat scenarios: 'an item, including a weapon, which either by design or through modification, is incapable of operating as a functional weapon'</li> </ul>	<ul style="list-style-type: none"> <li>General support as it will enhance security outcomes by exposing security screeners to a broader range of test weapons during system tests</li> <li>Test weapons should be either GPS tracked or clearly marked as a department test piece</li> </ul>	<ul style="list-style-type: none"> <li>Amending the definition in the initial approach to include the following caveat 'during the course of conducting a system test'</li> <li>Introducing a power to prescribe test weapons in the regulations</li> </ul>	<ul style="list-style-type: none"> <li>Updated definition: <ul style="list-style-type: none"> <li>'an item, including a weapon, which either by design or through modification, is incapable of operating as a functional weapon <i>during the course of conducting a system test</i>'</li> </ul> </li> <li>We support clearly marking test weapons as departmental test pieces</li> <li>Prescribing test weapons in the regulations will improve security outcomes by providing flexibility to include test pieces that reflect new and emerging threat scenarios. It also aligns with similar approaches undertaken by other government entities</li> </ul>

**Table 21: Responses to industry consultation**

No.	Measure	Initial approach	Industry feedback	Updated approach following consultation	Additional considerations
5	Introduce vulnerability testing	<ul style="list-style-type: none"> <li>Introduce vulnerability testing on Australian aviation security systems</li> <li>Vulnerability testing assesses equipment, people, and processes in an attempt to expose weaknesses by emulating an adversary who has both the intent and capability to exploit the security system</li> </ul>	<ul style="list-style-type: none"> <li>General support with information sought on the vulnerabilities it will test, the outcomes it seeks to achieve, how it will be delivered, and how disruptions will be minimised</li> <li>No support for vulnerability testing becoming a mandatory component of compliance testing</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial policy approach</li> </ul>	<ul style="list-style-type: none"> <li>Vulnerability testing will not be a compliance activity that results in enforcement action</li> <li>The department will develop a vulnerability testing program that will identify: <ul style="list-style-type: none"> <li>the security outcome seeking to be achieved</li> <li>how vulnerabilities are classed/identified</li> <li>how vulnerability tests will be delivered</li> </ul> </li> </ul>
6	Introduce maritime system and vulnerability testing	<ul style="list-style-type: none"> <li>Introduce system and vulnerability testing in the maritime sector</li> </ul>	<ul style="list-style-type: none"> <li>General support with information sought on how it will work in practice and be implemented</li> <li>Critical information and results should be shared with industry participants promptly so they can be addressed. Industry participants support the sharing of industry wide de-identified learnings</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial policy approach</li> </ul>	<ul style="list-style-type: none"> <li>Maritime system testing will initially be limited to the relevant screening point of passenger ships</li> <li>We will provide guidance on this measure, including on: <ul style="list-style-type: none"> <li>the security outcome seeking to be achieved</li> <li>how it may work in practice and be implemented</li> </ul> </li> </ul>
7	Special security directions (SSDs)	<ul style="list-style-type: none"> <li>Broaden SSD powers to include a specific, direct, or change in an existing general threat across all hazards</li> </ul>	<ul style="list-style-type: none"> <li>General support, noting directions need to remain measured and proportionate</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial policy approach</li> </ul>	<ul style="list-style-type: none"> <li>The SSDs will continue to be a last resort power, used in exceptional circumstances. This will be outlined in the explanatory memorandum</li> </ul>
8	Demerit points for air cargo	<ul style="list-style-type: none"> <li>This measure will provide the department with the power to implement a demerit point scheme in the air cargo sector in alignment with the broader aviation sector</li> </ul>	<ul style="list-style-type: none"> <li>Some industry participants questioned why the demerit points system is being extended when it is not currently being used, and sought clarification on its implementation</li> <li>Some industry participants enquired if points could be restored for industry participants who show positive security outcomes, details for grading systemic non-compliance, as well as advice on reviewing and appealing decisions</li> </ul>	<ul style="list-style-type: none"> <li>Proceeding with initial policy approach</li> </ul>	<ul style="list-style-type: none"> <li>Separate consultation with industry will take place if a demerit scheme will be implemented and as part of this we will provide details on how the demerit point system will work in practice, including on: <ul style="list-style-type: none"> <li>how we propose to achieve a fair and equitable scheme given the variation in size, operation, and complexity between industry participant</li> <li>point allocation, review/appeal options, and if points can be restored</li> <li>how the system will operate alongside other compliance powers</li> </ul> </li> </ul>

**Table 21: Responses to industry consultation**

No.	Measure	Initial approach	Industry feedback	Updated approach following consultation	Additional considerations
11	Protecting day to day maritime operations critical to Australian ports	<ul style="list-style-type: none"> <li>• Include harbour master operations as a maritime industry participant</li> <li>• Broaden the definition of 'security regulated port'</li> </ul>	<ul style="list-style-type: none"> <li>• Industry participants did not support the regulation of harbour masters</li> <li>• Most industry participants enquired about the specifics and unintended consequences of amending the definition of 'security regulated port'</li> </ul>	<ul style="list-style-type: none"> <li>• No longer proceeding with the amendment to regulate harbour master operations</li> </ul>	<ul style="list-style-type: none"> <li>• We will consult with relevant industry participants before security regulated port boundaries are amended, including whether land will be in scope</li> <li>• If new industry participants are identified, we will work alongside the entities to ensure they are aware of, and comply with, their security obligations</li> </ul>
14	Replace 'sex' with 'gender'	<ul style="list-style-type: none"> <li>• Replace 'sex' with 'gender'</li> <li>• Include in the regulations the caveat 'if practicable'</li> </ul>	<ul style="list-style-type: none"> <li>• General support with guidance sought on what the exemption means for screening procedures</li> </ul>	<ul style="list-style-type: none"> <li>• Proceeding with initial policy approach</li> </ul>	<ul style="list-style-type: none"> <li>• Screening officers will be required to make reasonable efforts to consider the individual's gender identity, and assign a screening officer accordingly for all frisk searches. The 'if practicable' exemption allows for situations where no screening officer of the same gender identity can be located</li> <li>• We will provide guidance on this measure, including on: <ul style="list-style-type: none"> <li>○ how officers may be guided to consider gender identity in a public setting and how to navigate scenarios where an officer of the same gender identity cannot be located</li> <li>○ how it will impact escort arrangements for persons in lawful custody</li> </ul> </li> </ul>

\*Note: measures 9, 10 and 15 are not included in this table as no feedback warranting government response was received.



### 5.2.3 Feedback received through consultation on the first pass IA

The first pass IA was released to industry for verification of its cost estimates on 17 October 2024, requesting written submissions be sent to the department by 24 October 2024. The department sought submissions from over 2000 stakeholders on the first pass IA, with 10 entities providing written submissions.

In general, the consultation feedback from industry on the first pass IA analysis was disparate. The department received 10 responses – 5 entities agreed with option 4 being the best option, 1 entity considered option 3 to be more reasonable and the remainder were unable or did not provide a view, citing additional information on specifics of the obligations was needed to form a view.

Respondents generally agreed that the cost split between obligations in option 4 and presented in table 14 were reasonable based on the information provided. However, the majority of responses were unable to verify whether the assessment of cost impacts and expected net benefits were reasonable. While generally supportive, several submissions noted that an absence of specific guidelines and regulations in relation to the proposed option 4 measures made an assessment of the reasonableness of costs difficult.

### 5.2.3 Evaluating regulatory impacts

For the reform proposals to achieve their goals, the department is committed to ensuring that the benefits of regulatory change outweigh any regulatory impact, while achieving the government's objectives. This requires understanding the full extent of regulatory impacts through a comprehensive IA assessment.

To supplement feedback received on the Consultation Paper, the department also sought to obtain views from industry on the financial impacts of the 15 measures set out in this document. The department received costing information from four industry participants, which has been incorporated into the cost benefit analysis contained in question 4 of this IA.

## 5.3 Future consultation

Recent incidents have highlighted the transport sector is vulnerable to a wide range of risks, including cyber security risks, supply chain disruptions, and natural hazards. Without mandatory all hazard security obligations, the transport sector will remain vulnerable to security threats, which would compromise the reliability, continuity and security of Australia's critical infrastructure. This would have subsequent impacts for Australia's prosperity and security, by disrupting essential services.

Expediting the introduction of the Bill, and the stronger security measures it contains, will help to address these threats. These measures are well-socialised with industry through specific consultation rounds and discussion at industry forums.

Given the compressed timeframes to introduce the Bill, we are unable to provide an industry with a draft Bill for consultation. The department will hold a town hall with industry to discuss the Bill text and upon request bilateral meetings with individual entities.

Future consultation and support with industry will also comprise:

- the distribution of guidance material on how the legislative frameworks are changing, which new obligations will apply to each cohort of entities, and some examples of how to best meet these obligations. The guidance material will also address common questions from previous rounds of consultation.
- Transport Security Reforms Advisory Committee meetings to discuss the development and progress of the reforms and discuss issues topical to industry participants.
- Consideration of the consequential amendments as they are progressed, including on all hazards security obligations, security controlled activities, maritime system testing, demerit points for air cargo, infrequent international vessels, dual purpose vessels and security regulated port definition.
- Consideration of any further rounds of reforms.

# 6. What is the best option from those you have considered and how will it be implemented?

## 6.1 Best option from those considered

The preceding consultation outcomes and analysis has demonstrated that option 4 – Amend ATSA, MTOFSA and their associated regulations to enact mandatory obligations, is the most suitable option from those considered.

Section 2 of this IA identified the objectives of government action. These objectives align with, and seek to address, the elements of the problem discussed in Section 1. Table 22 below demonstrates that amendments under option 4 will support each of the government’s objectives for intervention and comprehensively address the problems identified and discussed throughout this IA.



*Table 22: Assessment of option 4 against objectives and problem elements*

	What is the problem?	What are government’s objectives?		Why option 4?
1.1	There are a growing number of threats to Australia’s transport sector, including an increasing risk of cyber incidents	<ul style="list-style-type: none"> <li>• Ensure government and industry are equipped to respond to current and emerging threats</li> <li>• Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards security threats</li> <li>• Ensure Australia continues to comply with its international aviation and maritime security obligations</li> </ul>	✓	<ul style="list-style-type: none"> <li>• Addresses the frequency and impact of any disruption to Australia’s transport sector</li> <li>• Allows support from government to coordinate post incident responses and intervention where appropriate to mitigate the consequences of such incidents</li> <li>• Ensures government and industry are equipped to respond to current and emerging threats</li> <li>• Improves government visibility over risk management processes</li> <li>• Allows industry the flexibility in addressing and responding to evolving threats</li> </ul>

	What is the problem?	What are government's objectives?		Why option 4?
1.2	The dynamic and uncertain nature of these threats means the transport sector faces challenges in preparing for, mitigating, and responding to the realisation of these threats	<ul style="list-style-type: none"> <li>• Ensure government and industry are equipped to respond to current and emerging threats</li> <li>• Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards security threats</li> <li>• Ensure Australia continues to comply with its international aviation and maritime security obligations</li> </ul>	✓	<ul style="list-style-type: none"> <li>• Addresses the frequency and impact of any disruption to Australia's transport sector</li> <li>• Allows support from government to coordinate post incident responses and intervention where appropriate to mitigate the consequences of such incidents</li> <li>• Ensures government and industry are equipped to respond to current and emerging threats</li> <li>• Improves government visibility over risk management processes</li> <li>• Allows industry the flexibility in addressing and responding to evolving threats</li> </ul>

The summary contained in table 22 above indicates that option 4 is the best option. This is because option 4 is the only option capable of addressing each problem area identified in this IA. It achieves the objectives of government intervention and stands to deliver substantial benefits to industry and the Australian economy as a whole. Conversely, table 23 below draws on the analysis undertaken in Section 4 above, to highlight that options 1, 2, and 3 are unable to address the identified problem areas and meet government's objectives for intervention.

**Table 23** Assessment of options 1, 2, & 3 against objectives and problem elements

	What is the problem?	What are government's objectives?		Why not option 1, 2, or 3?
1.1	There are a growing number of threats to Australia's transport sector,	<ul style="list-style-type: none"> <li>• Ensure government and industry are equipped to respond to current and emerging threats</li> <li>• Ensure industry can meet desired security</li> </ul>	  	<p><b>Option 1:</b></p> <ul style="list-style-type: none"> <li>• Current problem elements will persist as the transport sector remains exposed to threats</li> <li>• Insufficient mitigations will maintain the potential for a security incident to occur</li> </ul> <p><b>Option 2:</b></p> <ul style="list-style-type: none"> <li>• Existing regulatory gaps are not addressed</li> </ul>

	What is the problem?	What are government's objectives?		Why not option 1, 2, or 3?
	including an increasing risk of cyber incidents	<p>outcomes, including through identifying, mitigating, and responding to all hazards security threats</p> <p>Ensure Australia continues to comply with its international aviation and maritime security obligations</p>	✘	<ul style="list-style-type: none"> <li>Potential additional costs associated with increased threats and entities choosing not to consider guidance material to uplift their risk mitigation strategies</li> <li>Government has limited visibility over industry's existing risk management practices</li> </ul> <p>Should one entity in the supply chain choose to not uplift their capability, it poses a risk to the whole supply chain despite any capability improvement made by other entities</p> <p><b>Option 3:</b></p> <ul style="list-style-type: none"> <li>Mitigating the problem elements through the SOCI Act will not capture the transport sector holistically</li> <li>Does not provide the government with adequate powers to enforce industry compliance</li> <li>Presents additional compliance burden on industry, having to respond to security obligations across multiple legislative frameworks</li> </ul>
1.2	The dynamic and uncertain nature of these threats means the transport sector faces challenges in preparing for, mitigating, and responding to the realisation of these threats	<ul style="list-style-type: none"> <li>Ensure government and industry are equipped to respond to current and emerging threats</li> <li>Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all hazards security threats</li> <li>Ensure Australia continues to comply with its international aviation and</li> </ul>	✘	<p><b>Option 1:</b></p> <ul style="list-style-type: none"> <li>Current problem elements will persist as the transport sector remains exposed to threats</li> <li>Insufficient mitigations will maintain the potential for a security incident to occur</li> </ul> <p><b>Option 2:</b></p> <ul style="list-style-type: none"> <li>Existing regulatory gaps are not addressed</li> <li>Potential additional costs associated with increased threats and entities choosing not to consider guidance material to uplift their risk mitigation strategies</li> <li>Government has limited visibility over industry's existing risk management practices</li> <li>Should one entity in the supply chain choose to not uplift their capability, it poses a risk to the whole supply chain despite any capability improvement made by other entities</li> </ul>

	What is the problem?	What are government's objectives?	Why not option 1, 2, or 3?
			<p><b>Option 3:</b></p> <ul style="list-style-type: none"> <li>• Mitigating the problem elements through the SOCI Act will not capture the transport sector holistically</li> <li>• Does not provide the government with adequate powers to enforce industry compliance</li> <li>• Presents additional compliance burden on industry, having to respond to security obligations across multiple legislative frameworks</li> </ul>

As demonstrated in table 23 above, options 1, 2, and 3 are not capable of solving the policy problem, nor aligning with the government objectives for intervention outlined by this IA. Without implementing option 4 as demonstrated in table 23 above, the identified problem areas cannot be addressed, government's objectives for intervention cannot be met, and industry and the Australian economy as a whole will not experience, to the full extent, the avoided costs outlined above.

### 6.1.1 Implementation

Although it offers the best option from those considered, option 4 is not without risks. Effective implementation of option 4 is essential for ensuring its benefits are realised in their entirety. The required implementation activities associated with option 4 are listed in table 24 and the risks to implementation and required management mitigations are discussed in table 27.

### 6.1.2 Approach to implementation

This section outlines the department's proposed implementation plan, including an outline of key implementation tasks, and the challenges or risks associated with implementing option 4. In line with the Government's Policy Impact Analysis guidance, evaluation considerations, including an evaluation plan, are contained in section 7 below. Government's objectives for implementation are to introduce option 4 in a manner which ensures affected industry stakeholders:

- understand and comply with their new or additional obligations under new regulatory requirements under option 4
- continue to engage with government to identify, understand and mitigate risks which exist in the sector, and collaborate to drive the implementation of strong security standards and expedient post-incident responses
- receive appropriate and consistent direction, assistance, and guidance from government, to allow for compliance with new and expanded obligations.

## Implementation plan

Effective implementation requires the completion of several key steps, identified below in Figure 3. Additional detail on these activities is set out table 24.

*Figure 3: Overview of implementation plan*



**Table 24: Detail on implementation activities**

Stage	Activities
Stage 1	<ul style="list-style-type: none"> <li>• Consideration and passage of legislative amendments captured under option 4</li> <li>• Circulation of guidance material for industry on compliance obligations, which may include:               <ul style="list-style-type: none"> <li>○ case studies</li> <li>○ frequently asked questions</li> <li>○ guidance and engagement through relevant industry forums</li> <li>○ insights into best practice and government’s expectations</li> </ul> </li> </ul>
Stage 2	<ul style="list-style-type: none"> <li>• Development and passage of supporting regulations, including an additional consultation period</li> </ul>
Stage 3	<ul style="list-style-type: none"> <li>• Commencement of transition period where industry commence undertaking activities to become compliant with the new regulatory requirements, for example, completing an all hazards risk assessment or reporting cyber security incidents</li> <li>• Education and engagement, including implementation of formal and informal regular feedback mechanisms, including through the TISN and open communication with the department</li> <li>• Preparation of policies and procedures for compliance activities</li> </ul>
Stage 4	<ul style="list-style-type: none"> <li>• Compliance and enforcement of expanded obligations commences</li> </ul>
Stage 5	<ul style="list-style-type: none"> <li>• Post-implementation review of amendments</li> </ul>

### Governance Arrangements

The department has implemented and will also develop and progress initiatives that will support the uplift of government and industry capability and partnerships, including consideration of appropriate governance arrangements.

The department will also continue to convene TSRAC meetings, to oversee and discuss key issues relevant to the development and implementation of the measures.

### Approach to compliance

The department specifies 5 principles which provide guidance in the exercise of its regulatory powers and engagement with critical infrastructure owners and operators.<sup>54</sup>

These principles inform the way in which the department’s regulatory function engagements with industry including, wherever possible, working in partnership with regulated entities to manage and understand risk. This approach reflects the department’s vision for voluntary legislative compliance by owners and operators and ultimately, the effective management of security risks across the transport sector.

<sup>54</sup> Regulatory principles and approach, CISC, 2024, [www.cisc.gov.au/legislation-regulation-and-compliance](http://www.cisc.gov.au/legislation-regulation-and-compliance)





**Table 25: Department's regulatory principles**

Principle	Meaning
Focus on risk	<ul style="list-style-type: none"> <li>Focus attention and resources on higher risk areas to ensure the resilience and security of the sectors we regulate</li> </ul>
Promote voluntary compliance	<ul style="list-style-type: none"> <li>Where appropriate, adopt a consultative approach with industry stakeholders</li> <li>Solicit feedback to inform continuous improvement within the aviation, maritime, and air cargo sectors</li> <li>Provide education and guidance to help industry understand their legislative obligations</li> </ul>
Be accountable, fair, and transparent	<ul style="list-style-type: none"> <li>Avoid unnecessarily impacting the efficient and effective operations of regulated entities, while making timely decisions based on legislative requirements</li> </ul>
Act consistently	<ul style="list-style-type: none"> <li>Deliver equitable decision-making across the aviation, maritime and air cargo sectors</li> </ul>
Act proportionately	<ul style="list-style-type: none"> <li>When exercising enforcement powers, we consider the:                             <ul style="list-style-type: none"> <li>security implications of non-compliance;</li> <li>seriousness of non-compliance;</li> <li>compliance history and regulatory posture of the entity;</li> <li>need for deterrence;</li> <li>facts of the matter at hand; and</li> <li>impact on Australia's reputation or Australian interests overseas</li> </ul> </li> </ul>

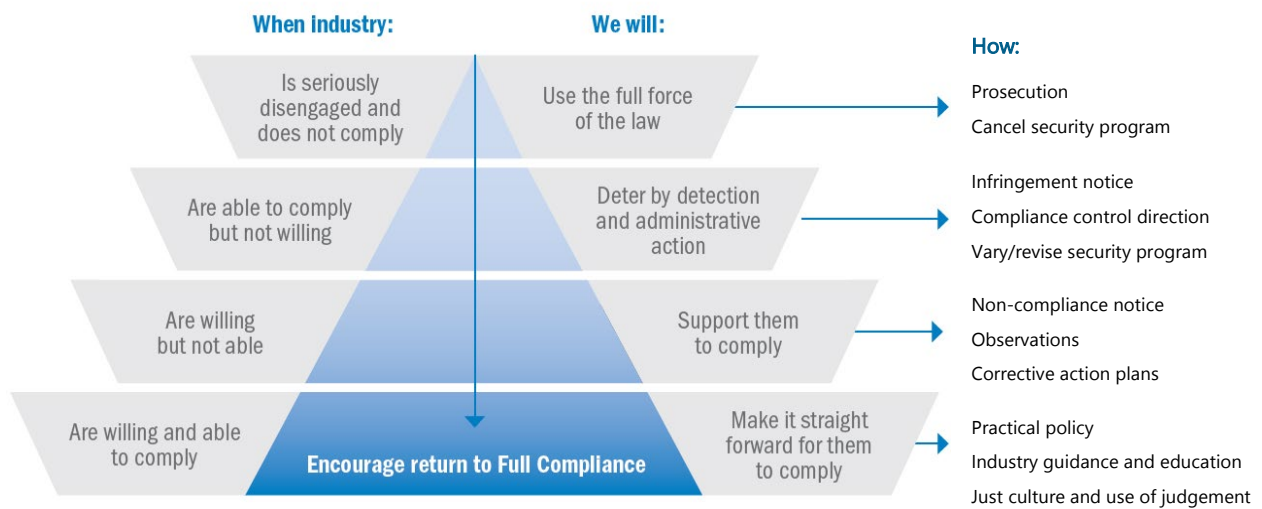
These principles inform the way in which the department's regulatory function engages with industry including, wherever possible, working in partnership with regulated entities to manage and understand risk. This approach reflects the department's vision for voluntary legislative compliance by owners and operators and ultimately, the effective management of security risks across the transport sector.

**Possible regulatory responses**

If industry participants fail to comply with their proposed legislative measures following their passage and the end of the transition period, they may be subject to a regulatory response. The department would work to educate and guide entities towards best practice security management, wherever possible, to encourage voluntary compliance. This would include educating responsible entities to ensure they understand their administrative and legislative obligations, as well as maintaining strong links with entities to promote ongoing best practice behaviours.

Figure 4 below outlines the department's proposed approach to imposing regulatory responses, in the event of non-compliance. The department would use a tiered approach to form its regulatory posture. Under this approach, regulatory actions and activities would be undertaken based on a scale ranging from support to penalties, proportionate to the nature and level of risk identified.

Figure 4: Regulatory options



When assessing non-compliance and determining an appropriate response, the department will consider the following 3 factors:

1. **Risk** - What is the impact of non-compliance on Australia’s national security? What is the nature of the risk? What solutions are available and how effective are they?
2. **Proportionality** - How serious is the risk? Are there any aggravating circumstances?
3. **Entity’s engagement** - What is the entity’s attitude towards compliance? How cooperative is the entity, based on engagement with the Department and their compliance history?

This approach will not impact on the transition period proposed by the department for expanded obligations which arise from the regulatory proposals contemplated in this IA.

### 6.1.3 Challenges and risks to implementation

There are several challenges and risks which could impede the department’s successful implementation of option 4. These challenges and risks are identified in table 27 below, and rated in terms of their likelihood and consequence, in accordance with table 26.

**Table 26: Likelihood and consequence ratings**

Likelihood		Consequence	
<b>Low</b>	The identified risk or challenge is unlikely to eventuate	<b>Minimal</b>	If the identified risk or challenge does eventuate, it would have a limited effect on the department’s ability to implement the proposed measures
<b>Medium</b>	It is reasonably possible that the identified risk or challenge will eventuate	<b>Moderate</b>	If the identified risk or challenge does eventuate, it would have a substantial effect on the department’s ability to implement the proposed measures
<b>High</b>	It is likely that the identified risk or challenge will eventuate	<b>Severe</b>	If the identified risk or challenge does eventuate, it would have a significant effect on the department’s ability to implement the proposed measures

Table 27: Challenges and risks to implementation

Identified risk	Likelihood	Consequence	Management	Residual risk
<p><b>Lack of industry awareness of amendments:</b> Some industry stakeholders may be unaware of the amendments, or the extent of their new obligations under ATSA and MTOFSA</p>	Low	Severe	<p>The department has prioritised engagement with industry to mitigate the existence of this risk. Engagement has included extensive consultation with industry (including town halls, round tables and open feedback forums) to provide context on the proposed reforms and eliciting feedback. There will also be ongoing communication with industry about the implementation of the reforms and resources available to support their transition (including on the department’s website).</p>	<p><b>Low:</b> It is unlikely that any affected entities would be unaware of the upcoming introduction of the reform measures to ATSA and MTOFSA, especially where ongoing support is provided to industry through the transition period.</p>
<p><b>Government capability:</b> Insufficient funding or understaffing could impact on the effectiveness of the proposed reforms, especially in relation to compliance activities</p>	Low	Severe	<p>Government has been regularly and comprehensively briefed on the developments of the proposed reform package, including requirements for compliance activities. This has allowed for identification of potential resources required to support implementation and evaluation activities.</p>	<p><b>Low:</b> Officials engaging with industry are knowledgeable, highly skilled at identifying vulnerabilities in the transport sector, and are able to support the department’s regulatory role.</p>
<p><b>Implementation costs:</b> There is a risk that the expected costs of</p>	Medium	Moderate	<p>Requesting that industry include a cost range when providing costing data has supported mitigation</p>	<p><b>Low:</b> The use of various data sources means any over or underestimation of the</p>

Identified risk	Likelihood	Consequence	Management	Residual risk
<p>implementation are either over or underestimated by industry and within this IA</p>			<p>of the risk that costs to industry could be higher than anticipated.</p> <p>Given the low number of costing templates received, this data has been supplemented by 2022 data attached to CIRMP obligations, and other data and academic resources. Together, these sources enhance the accuracy of the impact analysis contained in this document.</p>	<p>expected costs will be minimal.</p> <p>Further, the net benefit analysis has incorporated a cost range which accounts for the uncertainty about cost impact.</p>

# 7. How will you evaluate your chosen option against the success metrics?

## 7.1 Approach to evaluation

The effectiveness of the proposed amendments under option 4 will be assessed on an ongoing basis. This will include through Parliamentary processes and ad hoc feedback from industry and government stakeholders (including through mechanisms such as the TISN).

## 7.2 Indicators of success

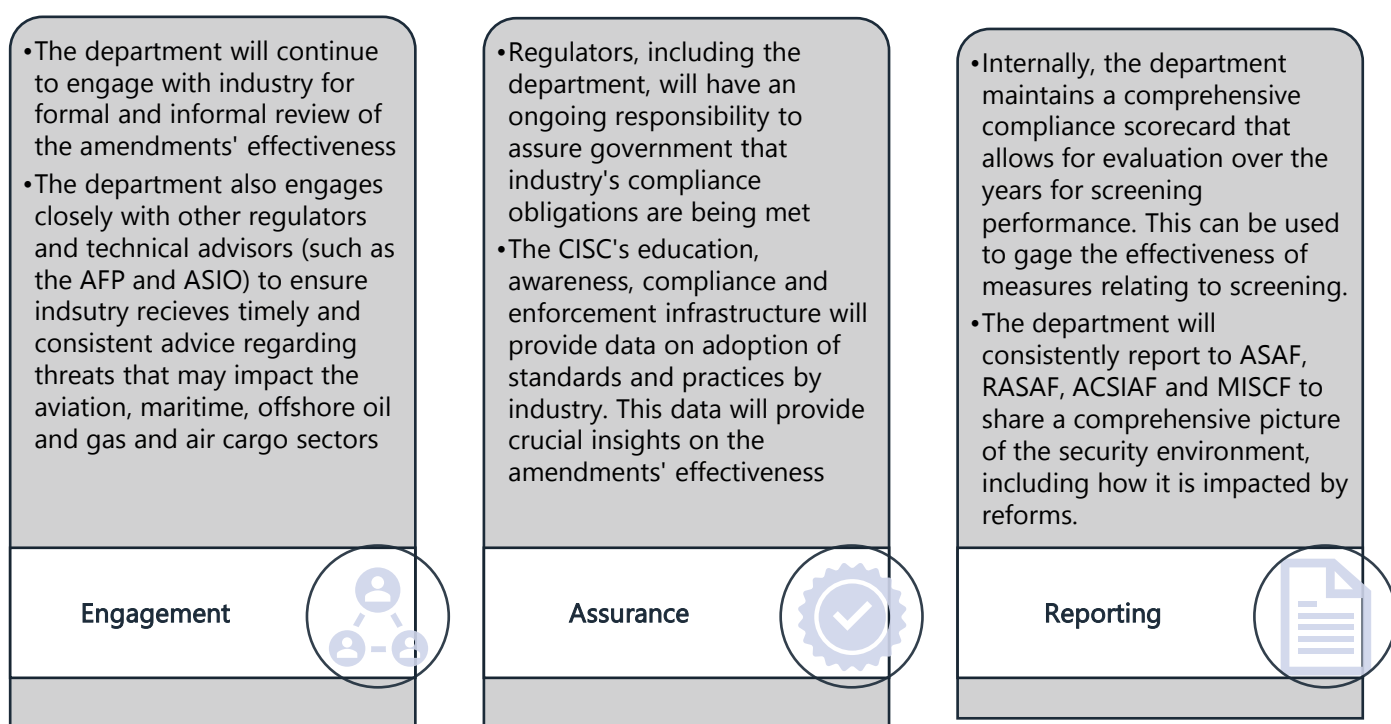


Figure 5 Evaluation mechanisms

The proposed regulatory amendments under option 4 will ensure that the transport sector can adapt and respond to current and emerging threats in a flexible, risk-based, and scalable manner.

If implemented successfully, the regulatory amendments under option 4 will:

- allow government, industry, and the Australian public to have ongoing confidence in the resilience of the transport sector as a key critical infrastructure sector
- ensure the provision of adequate support from government to industry in the aftermath of an incident
- foster a strengthened relationship between industry and government through heightened and more frequent engagement, knowledge, and awareness of the department's approach to compliance, and improved visibility for both industry stakeholders and government.

Section 2 outlined appropriate approaches to measure the reform objectives. The following metrics will guide the evaluation:

- Objective: Transport security legislative frameworks are robust, proportionate, and fit-for-purpose
  - Metric: Government’s ability to regulate in a flexible, scalable, risk-based way
    - Target: Entities are meeting security outcomes while also being regulated proportionately to its risk and operating environment
  - Metric: Entities are resilient to current and emerging threats
    - Target: Entities identify and effectively mitigate their security risks.
- Objective: Major security incidents in the Australian transport sector are minimised
  - Metric: Number of major security incidents in the Australian transport sector
    - Target: Reduction in number of major incidents in Australia
  - Metric: Ratio of major security incidents in Australia relative to incidents in other relevant economies
    - Target: Reduction in the ratio of incidents in Australia compared to overseas
- Objective: Disruptions to Australian transport operations caused by lapses in security are minimised
  - Metric: Scale of major security incidents in the Australian transport sector
    - Target: Reduction in the scale of major incidents in Australia
  - Metric: Ratio of major security incidents in Australia relative to incidents in other relevant economies
    - Target: Reduction in the ratio of average size of incidents in Australia compared to overseas

After the initial grace period during which the department’s focus would be education and engagement, the department may adopt its regular compliance approach. This would include issuing non-compliance notices and observation notices where compliance issues or vulnerabilities are identified. However, the severity of the enforcement action could increase to those industry participants who severely fail to implement the proposed requirements within the required timeframe or for egregious non-compliance. As depicted in table 28 below, the majority of effort should be directed towards ‘persuasion’ tactics, including education and engagement with industry.

The above indications of success align with government’s objectives for intervention, as outlined in table 28 below.



Table 28: Alignment between government objectives and outcomes

Government objectives	Indicator of success	Evidence of Success
<p>Ensure government and industry are equipped to respond to current and emerging threats</p>	<ul style="list-style-type: none"> <li>• Allow government, industry, and the Australian public to have ongoing confidence in the resilience of the transport sector as a key critical infrastructure sector</li> <li>• Ensure the provision of adequate support from government to industry in the aftermath of an incident</li> <li>• Foster a strengthened relationship between industry and government through heightened and more frequent engagement, knowledge, and awareness of the department’s approach to compliance, and improved visibility for both industry stakeholders and government</li> </ul>	<ul style="list-style-type: none"> <li>• Industry has the ability to clearly identify, implement and comply with international and domestic standards</li> <li>• Industry develops greater capability in the ways they can respond to all hazards security risks</li> <li>• There is a flexible and transparent approach to interactions with government, which builds relationships and includes leveraging government support where appropriate</li> <li>• There is a reduction in the number of (or severity of) attacks on aviation and maritime sectors arising through all hazards threats</li> <li>• There is a reduction in the number of (or severity of) impacts to Australian maritime and aviation sectors arising from world-wide events.</li> </ul>
<p>Ensure industry can meet desired security outcomes, including through identifying, mitigating, and responding to all</p>	<ul style="list-style-type: none"> <li>• Allow government, industry, and the Australian public to have ongoing confidence in the resilience of the transport sector as a key critical infrastructure sector</li> <li>• Ensure the provision of adequate support from government to industry in the aftermath of an incident</li> <li>• Foster a strengthened relationship between industry and government through heightened and more frequent engagement, knowledge, and awareness of the department’s approach to</li> </ul>	<ul style="list-style-type: none"> <li>• Industry has the ability to clearly identify, implement and comply with international and domestic standards</li> <li>• Industry develops greater capability in the ways they can respond to all hazards security risks</li> <li>• There is a flexible and transparent approach to interactions with government, which builds</li> </ul>

<p>hazards threats.</p>	<p>compliance, and improved visibility for both industry stakeholders and government</p>	<p>relationships and includes leveraging government support where appropriate</p> <ul style="list-style-type: none"> <li>• There is a reduction in the number of (or severity of) attacks on aviation and maritime sectors arising through all hazards threats</li> <li>• There is a reduction in the number of (or severity of) impacts to Australian maritime and aviation sectors arising from world-wide events.</li> </ul>
<p>Ensure Australia continues to comply with its international aviation and maritime security obligations</p>	<ul style="list-style-type: none"> <li>• Allow government, industry, and the Australian public to have ongoing confidence in the resilience of the transport sector as a key critical infrastructure sector</li> <li>• Ensure the provision of adequate support from government to industry in the aftermath of an incident</li> <li>• Foster a strengthened relationship between industry and government through heightened and more frequent engagement, knowledge, and awareness of the department’s approach to compliance, and improved visibility for both industry stakeholders and government</li> </ul>	<ul style="list-style-type: none"> <li>• Industry has the ability to clearly identify, implement and comply with international and domestic standards</li> <li>• Industry develops greater capability in the ways they can respond to all hazards security risks</li> <li>• There is a flexible and transparent approach to interactions with government, which builds relationships and includes leveraging government support where appropriate</li> <li>• There is a reduction in the number of (or severity of) attacks on aviation and maritime sectors arising through all hazards threats</li> <li>• There is a reduction in the number of (or severity of) impacts to Australian maritime and aviation sectors arising from world-wide events.</li> </ul>

# Appendix A: Description of measures in Option 4

## Measure 1: Expand the definition of unlawful interference

### Issue

The current definition of unlawful interference requires aviation and maritime industry participants (IPs) to manage and report acts or threats of unlawful interference within their physical boundary or geographical location. Broadly speaking, this captures unlawful acts that place any person, or the safe operation of an IP at risk, which includes but is not limited to:

- taking control of an aircraft, ship, or offshore facility through force or intimidation
- destroying an aircraft or ship that is in service, or destroying an offshore facility
- putting the safety of a regulated entity at risk by interfering with, damaging or destroying navigation facilities, communication systems or security systems
- committing an act, or causing any interference or damage, that puts the safe operation of, or the safety of any person at an airport, port, offshore facility, aircraft or ship at risk.

This narrow focus does not adequately reflect the range and scale of threats facing IPs, the vector by which a threat may arise, or that threats are no longer limited to physical boundaries. Retaining the current definition would leave such threats largely outside the transport security regulatory purview, meaning IPs are not explicitly required to mitigate contemporary risks such as cyber threats or natural hazards.

### Proposal

The Government proposes to integrate risks arising from current and emerging all hazard threats, such as cyber, into the unlawful interference definition of the transport security legislative frameworks. This will maximise the effectiveness and preparedness of industry to meet the needs of the evolving threat environment. This proposal includes:

- expanding the definition of unlawful interference to capture a variety of acts, including cyber security incidents that has or is likely to have a relevant impact on aviation or maritime assets
- expanding reporting requirements to capture cyber security incidents under ATSA and MTOFSA, and attempted acts of unlawful interference for MTOFSA (excluding attempted cyber security incidents)
- removing the reference to 'terrorist acts' in the definition of a security incident in MTOFSA, to recognize the wide variety of hazards facing the transport sector.

## Measure 2: All hazards security framework

### Issue

Under the transport security legislative frameworks, certain IPs are required to have an approved security program describing mitigation measures they will implement to protect their infrastructure, assets and operations against unlawful interference and serious crime.

The introduction of an all hazards security framework seeks to ensure IPs are adequately protected against current and emerging threats, and align the security obligations and resilience of the transport sector with other critical infrastructure sectors regulated under the SOCI Act.

### Proposal

The Government proposes to introduce all hazard security obligations in the transport security legislative frameworks to ensure regulated IPs identify and mitigate all hazards risks relevant to their operating environment.

All hazards captures the spectrum of risks facing modern critical infrastructure IPs and comprises five areas:

- physical security (existing obligation under the transport security legislative frameworks)
- personnel security (existing obligation under the transport security legislative frameworks, but to be added to)
- cyber security
- supply chain security
- natural hazards.

IPs will be subject to individual all hazards obligations based on their unique operating environments and size, as outlined in Appendix B.

As part of this measure there will also be an introduced requirement for IPs to complete an all hazards risk assessment, and attestation, which will sit alongside an IP's SP.

### Additional obligations

#### *All hazards risk assessment*

The all hazards risk assessment will be submitted alongside your SP. This will be used to inform the regulator's assessment of the SP. For aviation IPs (AIPs), an all hazards risk assessment will replace the risk context statement you current submit. For maritime IPs (MIPs), an all hazards risk assessment will replace the security assessment you currently submit

It is intended that the all hazards risk assessment will model the security assessment details provided in the Maritime Transport and Offshore Facilities Security Regulations 2003 (MTOFSR) with the addition of an explicit requirement to consider risks in the all hazards categories. This includes:

- a statement outlining the risk context of the entity

- identification and details on the scope of the assets, infrastructure and operations being assessed
- identification and possible risks or threats to these assets arising from all hazards domains, and the likelihood and consequences of their occurrence
- identification of existing security measures, procedures and operations; identification of the gaps in security arrangements including gaps arising from all hazards domains, infrastructure, policy and procedures and
- identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

*Personnel security obligations:*

1. Outline processes to minimise or eliminate risks arising from a malicious or negligent employee or contractor during their employment, as well as implement an off boarding process for outgoing employees and contractors
2. Identify SCAs within an IP's entity and mitigate risks with personnel undertaking SCAs. This includes:
  - identifying through a risk assessment, SCAs within an IP's organisation. SCAs are activities that allow personnel to remotely have access to, or influence of, secure areas, security information or critical systems. This includes activities undertaken by international personnel and third party and subsequent suppliers
    - It should be noted there will be no prescriptive list of SCAs provided by the government, as activities within individual entities are contextual to each IP's business and operating model. IPs will be required to self-identify SCAs within their entity based on their operating model and operating and threat environments.
    - The government can provide guidance on what types of activities may be considered SCAs. For instance, IPs can consider the essential components or systems of their operations and who has responsibility of, access to, control over or management of these assets. In practice SCAs could include activities that have access to, or control of operations relating to operational technology and data systems, control operations of operational technology or HR information or processes.
  - implementing adequate mitigation measures to manage risks associated with personnel undertaking SCAs, including, where appropriate:
    - requiring relevant personnel to hold an ASIC/MSIC and/or
    - implementing relevant processes or procedures to ensure the security of relevant areas, information and systems. This may include an attestation from an international entity or third party supplier that personnel they engage supports an IP's obligation to meet desired security outcomes

- attesting the mitigation measures implemented, including the engagement of international personnel or third party suppliers, aligns with an IP's obligation to meet desired security outcomes.

More information on SCAs is provided in measure 3.

### *Cyber security obligations*

1. Minimise cyber risks, and mitigate their impact by complying with the most recent edition of one of the below cyber standards, or an equivalent framework:
  - Australian Standard ISO/IEC 27001
  - at a minimum, maturity level one of the Australian Signal Directorate's Essential Eight Maturity Model
  - meet Security Profile 1 of the 202021 AESCSF Framework Core published by Australian Energy Market Operator Limited (ACN 072 010 327)
  - US National Institute of Standards and Technology's Cyber Security Framework
  - meet Maturity Indicator Level 1 of the Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America

The framework or standard adopted should be outlined in the SP, and should be proportionate to the assessed risk. Older versions may be considered an equivalent framework so long as efforts to recertify to the most recent edition can be demonstrated. Overlapping combinations of numerous frameworks may be considered an equivalent framework.

2. Establish processes to protect critical systems and data

### *Supply chain security obligations*

1. Identify supply chain hazards that could significantly impact the IP or its operations
2. Identify major suppliers that by the nature of the product or service they offer, have a significant influence over the security of the IP's operations.
3. Establish processes to minimise or eliminate risks and impacts arising from:
  - unauthorised access, interference, or exploitation of the IP's supply chain
  - misuse of privileged access by any provider in the supply chain
  - disruption of the IP due to an issue in the supply chain
  - material risks associated with a major supplier in a supply chain
  - any failure or lowered capacity of other assets in the IPs supply chain.

### *Natural hazards obligations*

1. Outline processes to minimise risks arising from natural hazards on the regulated IP, and mitigate against its physical impacts and effects.

### *Attestation*

The attestation will be submitted alongside the all hazards risk assessment and the SP as an overarching assurance. Attestations will occur at least annually, or when the risk assessment or SP is amended, to verify that the risk assessment has been reviewed and is still accurate.

## **Measure 3: Security controlled activities measure**

### **Issue**

The transport security legislative frameworks currently focus on authorisation for access to physical security zones. Unescorted access to these zones are restricted to individuals who hold an ASIC or MSIC that have an operational need to be in the zone.

Rapidly evolving technology has enabled security zone operations once physically delivered to be delivered remotely. As a result, there are individuals who can affect, or influence, a secure zone, or critical systems, without being physically present within the border or geographical location of the entity.

### **Proposal**

The Government is proposing to:

- introduce a definition of SCAs within ATSA and MTOFSA, which refer to activities that can allow personnel to have access to, or influence of, secure areas, or critical systems, remotely
- introduce a requirement for IPs to identify SCAs through a risk assessment. This includes activities undertaken by international personnel and third party and subsequent suppliers
- introduce a requirement for IPs to implement mitigation measures to manage risks associated with personnel undertaking SCAs, including, where appropriate:
  - requiring relevant personnel to hold an ASIC/MSIC; and/or
  - implementing relevant processes or procedures to ensure the security of critical systems.

For any internationally-based personnel, including third party supplier located internationally, IPs are not required to obtain background checks outside of Australia. Under this measure, IPs will need to satisfy themselves, and provide an attestation that any internationally-based personnel or international third-party suppliers engaged by your entity, contribute to meeting your security obligations.

Your risk assessment and SP should also identify how your entity will mitigate any real or perceived risks and threats from internationally-based staff or international third-party suppliers.

# Appendix B: All hazard obligations by entity

The table below provides a proposed breakdown of all hazard obligations by entity.

Industry Participant	Personnel	Cyber	Natural hazards	Supply chain
<b>Aviation</b>				
Airservices Australia	✓	✓	✓	✓
Designated airports	✓	✓	✓	✓
Tier 1 airport	✓	✓	✓	✓
Aircraft operators operating regular public transport (RPT) services	✓	✓	✓	✓
Registered Air Cargo Agents (RACAs) operating at designated/tier 1 airports	✓	✓	✓	✓
Australian aircraft operators operating airfreight services at designated and tier 1 airports	✓	✓		✓
Tier 2 airports	✓	✓	✓	
Operators of airfreight services not captured as Australian operators in ATSA	✓	✓		
Tier 3 airports	✓			
Accredited air cargo agents (AACAs)	✓			
RACAs operating at only tier 2, Essendon, and Bankstown airports	✓			
Known consignors (KCs)	✓			
<b>Maritime</b>				
Port Operators	✓	✓	✓	✓
Port facility operators	✓	✓	✓	✓
Ship operators	✓	✓	✓	✓
Offshore facility operators	✓	✓	✓	✓
Offshore service providers	✓	✓	✓	✓



# Appendix C: List of acronyms

Acronym	Meaning
ASD's ACSC	Australian Signals Directorate's Australian Cyber Security Centre
ASIC/MSIC	Aviation/maritime security identification card
ATSA	<i>Aviation Transport Security Act 2004</i>
ATSR	Aviation Transport Security Regulations 2005
CIRMP	Critical Infrastructure Risk Management Program
CISC	Cyber and Infrastructure Security Centre
DDoS	Distributed Denial of Service
Independent Review	Independent Review into Australia's Aviation and Maritime Security Settings
MTOFSA	<i>Maritime Transport and Offshore Facilities Security Act 2003</i>
MTOFSR	Maritime Transport and Offshore Facilities Security Regulations 2003
SOCI Act	<i>Security of Critical Infrastructure Act 2018</i>
SCA	Security controlled activities
SSD	Special security direction
Transport sector	Aviation, maritime and offshore facility sectors
Transport security legislative frameworks	ATSA, ATSR, MTOFSA, MTOFSR