

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 1**

**Subject: Consultation to inform the design of the subsequent regulatory instruments**

***Asked by:*** Raff Ciccone

***Question:***

Does Home Affairs intend to conduct consultation to inform the design of the subsequent regulatory instruments that will be necessary to give effect to certain elements of the Bill and if so, what will that consultation process involve?

***Answer:***

The department is committed to undertaking a multi-faceted consultation approach that centres on engagement (informing, consulting, involving and collaborating) with key stakeholders to inform the design of subsequent regulatory instruments necessary to give effect to certain elements of the Bill. This includes:

- consulting with key stakeholders to ensure those who are impacted by, and have relevant expertise on, the reforms can inform its development and implementation. This includes:
  - relevant internal departmental areas who have policy or operational responsibility
  - relevant Commonwealth, state, and territory governments, including to ensure that any security obligations we progress are complementary to their frameworks, rather than duplicative
  - aviation, maritime, and offshore facility industry participants (the transport sector)
  - industry peak bodies
  - like-minded international partners
- engaging with stakeholders through a range of forums, including through:
  - transport sector town halls to allow the department to gauge broad views and interplays between the sectors; sector-specific meetings and workshops; bilateral meetings; and direct communication
  - regular department hosted industry forums, including the aviation security advisory forum, the regional aviation security advisory forum, the air cargo security advisory forum, the maritime industry security consultative forum and the strategic aviation security meeting

- industry hosted forums that the department is invited to attend such as the Australian Airports Association Divisional Meeting we attended during development of the TSA
- Bi-lateral meetings with an industry participant or participants to address specific regulations or impacts
- the transport security reforms advisory committee, established by the department in 2024, to provide strategic advice to the department on the development, and implementation of the transport security reforms. The Committee comprises co-chairs from each industry forum as well as industry representative bodies
- written documents, including sharing consultation papers and inviting written submissions
- communicating key messages, including project information and progress, consultation outcomes, and key decision points and outcomes.
- education, providing industry with guidance material to clearly define the new obligations, and how they will work in practice.

The development of the regulatory amendments will be an iterative process, with several opportunities for stakeholders to provide feedback. This will allow government and industry to work together to develop fit-for-purpose and robust legislative frameworks.

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 2**

**Subject: Competing goals of Home Affairs' functions**

**Asked by:** Raff Ciccone

**Question:**

Home Affairs is both the regulator and the policy lead on transport security— how have the competing goals of these two functions been balanced?

**Answer:**

A single department has been both regulator and policy lead on transport security since the aviation and maritime security legislation was introduced 20 years ago, originally in the (now) Department of Infrastructure, Transport, Regional Development, Communications and the Arts, and then in Home Affairs since it was established in 2017.

Having both the regulatory and policy functions co-located within the one department has been complementary. It has enabled:

- a deeper understanding of the legislative and policy framework, by the regulator
- a deeper understanding of the effectiveness of the regulatory policy framework and how it works in practice, and
- better collaboration and communication, especially during time of heightened threat.

The dynamic nature of the threats and hazards faced by the transport sector means there is a need for the regulator to understand the risk environment and what available controls exist to mitigate risks. A strong risk assessment and policy function, alongside the regulator, is key to understanding the threat environment, developing appropriate security standards, and ensuring the regulatory regime and toolkit is fit for purpose.

An integral aspect of balancing the interplay between the regulatory and policy functions is having a shared understanding of the department's regulatory role, focus and contribution. To assist with this, the department is refining:

- a regulatory position statement that will articulate the regulator's role, functions and focus
- a more granular compliance and enforcement policy to provide clear direction and support to internal teams to utilise the complete regulatory toolkit to achieve regulatory outcomes and minimise harm, and provide a basis for delivery and consistency

- its regulatory priorities to help better direct regulatory and policy resources across key harms, issues or priorities and support more targeted effort and investment

The department is also subject to external oversight and scrutiny by the Australian National Audit Office.

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 3**

**Subject: Scalability of the legislation**

**Asked by:** Raff Ciccone

**Question:**

How is it intended for this legislation to be made scalable?

**Answer:**

The Department fully recognises that each aviation and maritime industry participant is different, and one size most definitely does not fit all.

Regulatory security requirements already differ between airports based on allocated tier (which takes into account passenger volumes, operating environment and risk). The Bill takes this same principle of proportionate legislation and extends it further for all hazards, supply chain and cyber risks. Under the Bill and subsequent regulations, it is the Department's intent that industry participants will be subject to regulatory requirements that are proportionate to their type and scale of operations, as well as their importance to Australia's aviation and maritime sectors productivity, security, and prosperity.

In developing how the obligations should be scaled, consideration is being given to the potential impost to the industry participant of complying with the obligation(s), and whether the obligation for that class was necessary to enhance the overall security of the transport sector. This can be achieved through further consultation with industry as the regulations are developed.

For example:

- Tier 2 airports (typically regional security controlled airports that conduct security screening) will be required to complete a risk assessment, identify and mitigate additional personnel security obligations (security controlled activities), risks posed by cyber security incidents, and natural hazards. This will include maintaining compliance with an established cyber security framework, and identifying and implementing measures to protect critical systems. These obligations are proportionate to the operations of the asset.
- Tier 3 airports (regional and remote airports that are security controlled but do not conduct security screening), along with accredited air cargo agents (AACA), known consignors (KC), and registered air cargo agents (RACA) operating at only tier 2, and Essendon and Bankstown, airports will only be subject to additional personnel security obligations (security controlled activities) and risk assessment requirements.

To ensure that this scalability is built in, the legislation has been developed using a broad, principles based approach. The Bill prescribes the general matters that aviation and maritime entities need to account for in their security planning and arrangements, such as the requirement for security assessments as part of transport security programs. The subsequent regulations will operationalise these general requirements for different entities, providing options and flexibility to ensure that industry participants at different tiers are not adversely impacted but will be subject to requirements that suit their stature.

For a full detail of which proposed obligations apply to which entities, please see the table on page 4 of the attached guidance.



## Resilient to current and emerging threats

### All hazards security framework

Introduce all hazards security obligations under the transport security legislative frameworks

#### What is 'all hazards'?

Aviation and maritime IPs are currently required under the transport security legislative frameworks to have an approved SP describing the measures and procedures they will implement to secure their operations from **unlawful interference**.

Unlawful interference is limited to a list of acts committed or attempted to be committed. The purpose is to capture the **lack of lawful authority** behind this interference.

'**All hazards**' is the collective term used by the Australian Government to capture current and emerging security risks to critical assets.

Security risks associated with all hazards comprise: **Physical, personnel, cyber, supply chain, and natural hazards** risks.

**Operational interference** will cover acts, or the occurrence of hazards, which cause a **relevant interference** with the operations of an entity and materialise lawfully (for example, by way of accident or negligence).

When considering **relevant interference**, IPs must consider whether there has been interference (direct or indirect) with the availability, integrity, or reliability of an asset or operation, the confidentiality of information about or stored in an asset, or the confidentiality of information relating to an IP's operation.

Obligations will be set out in the regulations, on which we will consult you. New obligations will be subject to a 12 month transition period following the passage of regulatory amendments.

#### Why an 'all hazards' approach?

The security environment is complex, challenging and evolving. Government and industry must contend with protecting Australians and their interests against a broad spectrum of hazards, threats, and an increasing sophistication of attacks.

With the introduction of operational interference and all hazards security obligations, certain aviation and maritime IPs will be required to take a holistic and proactive approach towards identifying and mitigating all hazards security risks that could interfere with their business operations.

Both international and domestic assets that, if degraded, could interfere with an business operations, should be included in your security assessment against the risks that may impact them.

A robust SP that mitigates all hazards security risks relevant to your entity will enable you to:

- continue to provide your essential services upon which our communities and economy rely
- recover quicker from incidents that interfere with your critical asset
- enhance your entity's ability to protect your business from current and emerging threats.

The all hazards security framework builds upon your existing security obligations.

Security obligations	New or existing
Physical security	Existing
Personnel security	Existing, will be expanded to include security controlled activities
Cyber security	New
Supply chain security	New
Natural hazards	New



## Resilient to current and emerging threats

### All hazards SP package

Under this measure, regulated IPs will be required to conduct a security assessment, an SP, and provide a statement of compliance (attestation). Please see page 12 for a diagram outlining the existing, and new approach.

The details of the all hazards security package will be contained in future regulatory amendments. Once finalised, the regulatory amendments will be subject to a 12 month grace period. Guidance will be provided on how to complete both components. The department will undertake additional consultation on both.

#### 1. Security assessment



The security assessment will be submitted as part of the SP. This will be used to inform the regulator's assessment of the SP.\*

For aviation IPs (AIPs), the security assessment will replace the risk context statement you currently submit.

For maritime IPs (MIPs), your security assessment requirements will now consider all hazards security risks.

##### The security assessment will include:

- a statement outlining the risk context of the entity
- identification and details on the scope of the assets, infrastructure, and operations assessed
- identification of possible risks or threats to these assets arising from the all hazards areas, and the likelihood and consequences of their occurrence
- identification of existing security measures, procedures and operations; and the gaps in these including gaps arising from all hazards areas, infrastructure, policy and procedures
- identification, selection, and prioritisation of possible risk treatments (e.g. counter-measures and procedural changes to be implemented) and their effectiveness in reducing risks and vulnerabilities.

#### 2. Contents of the SP



Your SP will outline the measures and procedures you implement to mitigate risks posed by all hazards. The inclusion of your measures and procedures will commit you to maintaining them and make them enforceable, once the SP is approved.

#### 3. Statement of compliance



The statement of compliance will initially be submitted with the security assessment and SP as an overarching assurance.

Statements of compliance will then be re-submitted at least annually (within 90 days of anniversary), or when the security assessment or SP are amended, to verify they have been reviewed and are still fit-for-purpose.

##### The statement of compliance will attest that the information in the security assessment and the SP:

- appropriately considers all relevant transport security hazards and risks to your operating and threat environment
- outlines proposed control measures which address the identified risks, meet legislative requirements, and are within your entity's agreed risk tolerance
- identifies security controlled activities and mitigates their associated risks, including where the activities are occurring internationally.

The statement of compliance will replace the statement of undertaking (ATSR 2.05).



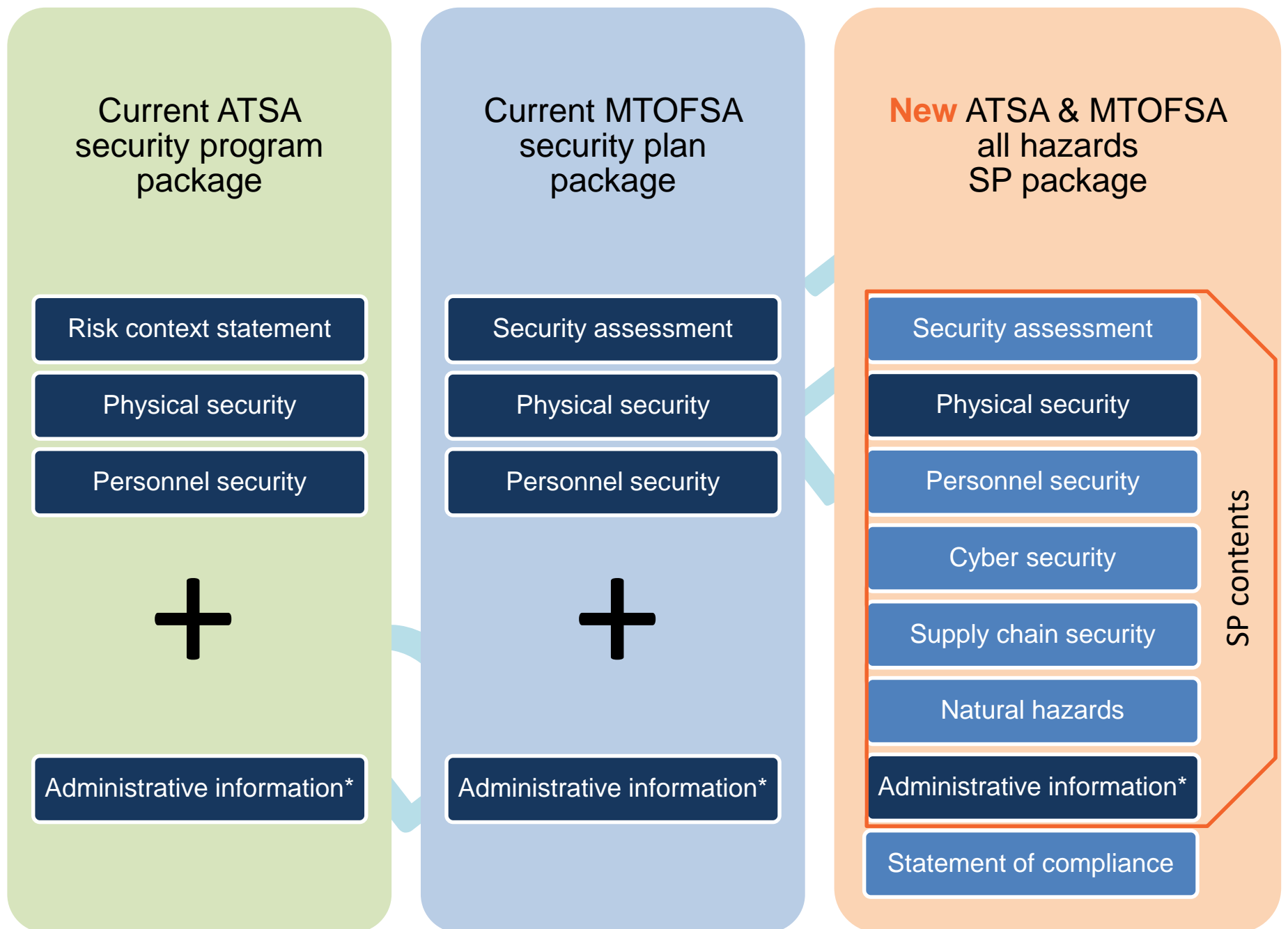


## Transport Security Reform: Legislative Package

### Current SP vs. new all hazards SP package

Currently, entities are required to submit an SP with the measures and procedures you implement to mitigate unlawful interference.

Under this measure, you will be required to submit an all hazards SP package comprising three elements – 1. a security assessment, 2. an SP, and 3. a statement of compliance.



\***Administrative information** includes information such as maps, security officer information, audit information and special event zones.

#### Key

Existing requirement
New requirement

The information contained in this document is general in nature and does not constitute legal advice. Industry participants are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.



Transport Security Reform: Legislative Package

All hazards security obligations by cohort

Industry participant	Security assessment	Statement of compliance	Physical	Personnel	Cyber security	Natural hazards	Supply chain
Aviation							
Air Services Australia	✓	✓	✓	✓	✓	✓	✓
Designated Airports	✓	✓	✓	✓	✓	✓	✓
Tier 1 Airports	✓	✓	✓	✓	✓	✓	✓
Aircraft Operators operating regular public transport services	✓	✓	✓	✓	✓	✓	✓
Regulated Air Cargo Agents (RACAs) operating at Designated or 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 the ATSA	✓	✓	✓	✓	✓		
Tier 3 Airports	✓	✓	✓	✓			
Accredited Air Cargo Agents (AACAs)	✓	✓	✓	✓			
RACAs operating at only Tier 2, Essendon, and/or Bankstown airports	✓	✓	✓	✓			
Known Consignors (KCs)	✓	✓	✓	✓			
Maritime							
Port Operators	✓	✓	✓	✓	✓	✓	✓
Port Facility Operators	✓	✓	✓	✓	✓	✓	✓
Ship Operators	✓	✓	✓	✓	✓	✓	✓
Offshore Facility Operators	✓	✓	✓	✓	✓	✓	✓
Offshore Service Providers	✓	✓	✓	✓	✓	✓	✓

The information contained in this document is general in nature and does not constitute legal advice. Industry participants are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.



## Resilient to current and emerging threats

### Personnel security, including security controlled activities (SCAs)



#### Proposed obligations (to be specified in the regulations)

- Outline processes to minimise or eliminate risks arising from a malicious or negligent personnel during their employment, and implement an off-boarding process for outgoing employees and contractors.
- Identify SCAs within your entity and mitigate risks with personnel undertaking SCAs.

#### Security controlled activities

SCAs are activities that allow personnel to remotely access or influence secure areas, security information, or critical systems. This includes activities undertaken by international personnel and third-party suppliers.

IPs are not required to obtain background checks outside of Australia for internationally-based personnel, including third-party suppliers located internationally.

Under this measure, IPs will need to satisfy themselves, and provide assurance within their statement of compliance that any internationally-based personnel or third-party suppliers engaged by your entity contribute to meeting your security obligations.

#### Mitigation measures

Measures to mitigate real or perceived risks associated with personnel undertaking SCAs must be identified within your security assessment and your SP.

Your SP should establish an evaluation framework that includes threat indicators, data profiles, and behavioral signals. This should be included in all phases of a personnel's work cycle: pre-employment, employment, and termination/post-employment.

#### Mitigation measures may include:

- requiring relevant personnel to hold an Aviation Security Identification Card or Maritime Security Identification Card (ASIC or MSIC)
- verifying the accuracy of resumes, contacting references, and screening for potential negative indicators during the interview process
- conducting routine, mandatory insider threat, physical, and cyber security awareness training
- communicating organisational policies and establishing baseline of normal behavior for both employees and information technology (IT) networks to identify significant changes, including monitoring network activity for dangerous or inappropriate activity
- identifying and reporting concerning behavioral changes to the appropriate security team/manager
- having established procedures to terminate outgoing personnel's physical and IT access, and informing other employees when personnel cease employment
- establishing the need-to-know principle, where access is only granted to a user if the information is immediately needed to perform a task
- ensuring technical controls are in place, such as multifactor authentication
- requiring an attestation from an international entity or third-party supplier that personnel it engages support an IP's obligation to meet desired security outcomes.

There will be **no prescriptive list of SCAs** provided by the department, as activities are contextual to each business and operating model.

**We provide examples of SCAs on the next page.**

Entities will be required to self-identify SCAs within their entity and appropriate mitigation measures based on their operating model and threat environments.



## Transport Security Reform: Legislative Package

### Examples of security controlled activities

Access to / control of	Risk	SCA personnel examples
Operations & automation of operational technology	Using operations and access to sensitive information to pose an insider threat	<ul style="list-style-type: none"><li>• crane and straddle operators and their managers</li><li>• yard managers and those who control vehicle movements through facilities</li><li>• airport or airline workers with access to operational technology</li><li>• engineers or maintenance workers who service operational technology</li></ul>
Human resources (HR) information or processes	Influencing the recruitment and movement of trusted insiders	<ul style="list-style-type: none"><li>• recruitment, HR staff and management who operate outside an airport/port</li><li>• management, security contractor staff who control rostering, and trucking companies who may influence rostering</li></ul>
IT and data systems associated within regulated entities	Control or compromise a system to access and/or use secure data for reasons relating to unlawful interference and/or serious and organised crime	<ul style="list-style-type: none"><li>• IT workers who have access to and/or influence over information or enabling IT systems</li><li>• those who have access to baggage and cargo systems</li><li>• those who control access systems which facilitate vehicle movements through facilities</li><li>• staff who do not operate in secure zones, but have access to cargo</li></ul>
Sensitive operational information	Access to and/or control of information which, if misused, could pose an insider threat	<ul style="list-style-type: none"><li>• logistics staff, managers, and anyone with access to container information or Australian Border Force flagged shipments</li><li>• truck drivers and trucking companies who access container information</li><li>• freight forwarders and cargo reporters with access to Integration Cargo System</li><li>• load control operators involved in the movement of baggage and cargo onto aircraft</li><li>• staff involved in the design of security policies and procedures in secure areas</li><li>• staff employed by screening providers with access to sensitive information</li></ul>
Other roles outside of a secure zone that may impact aviation or maritime security	Access to a secure zone and/or access to items used in a secure zone that may impact aviation or maritime security such as cargo, catering, or maintenance supplies	<ul style="list-style-type: none"><li>• security staff who protect assets which are not inside secure zones</li><li>• provedores, maintenance staff, mechanics, cleaners, or fumigators who do not operate in secure zones but still have access</li><li>• corporate roles relating to airports including freight, engineering, off-airport catering, maintenance, and ground services</li><li>• truck drivers who can access cargo not stored within a facility in a secure zone</li><li>• train driver and rail workers within or next to a port facility involved in moving and loading cargo and freight</li><li>• cargo examining aircraft operators</li><li>• finance-related roles, including property and procurement</li><li>• corporate compliance officers and investigators</li></ul>

The information contained in this document is general in nature and does not constitute legal advice. Industry participants are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.





## Resilient to current and emerging threats

### Cyber security



#### Obligations to be specified in the Regulations

1. Requirement to 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 pending the department's agreement:
  - [Australian Standard AS ISO/IEC 27001](#)
  - Meet maturity level one of the [Essential Eight Maturity Model published by the Australian Signals Directorate](#)
  - [Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States of America](#)
  - Meet maturity level one of the [Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America](#)
  - [The AESCSF Framework Core published by Australian Energy Market Operator Limited \(ACN 072 010 327\)](#).
2. Establish processes to protect critical systems and data.

### Identification of a cyber security framework

The cyber security framework your entity is complying with should be set out within your SP (for example, within either the Quality Control or Information Security sections, or as an annexure).

IPs may use an existing cyber security framework or relevant excerpts to meet this requirement if it includes adequate measures in place to protect critical systems and data, pending the department's agreement.

### What is an equivalent framework? How do you maintain a recent edition?

Entities should consider their risk management methodology and the cyber risks most relevant to their asset when considering implementing cyber security frameworks not listed in the regulations.

If an alternative framework is more appropriate to your business operations, the department may consider this a valid equivalent framework. The department is keen to proactively engage with entities considering implementing alternative frameworks.

If your entity achieves cyber security through numerous frameworks, or overlapping components of numerous frameworks, the department may consider this an equivalent framework, if it can be clearly demonstrated in your submission and each framework complies with desired security objectives.

Continuously monitoring the frameworks you choose for updates will be the responsibility of the IP. When a new edition is released, you must be compliant with the updated framework as soon as possible, within 12 months of the new edition being released.

### Protection of critical systems and data

This requirement seeks a description of the measures to protect the identified critical systems and data relevant to your operations. Further information is on page 16.

You must clearly describe how your critical systems and data are being protected in your SP. Generic statements such as 'password security' and 'multifactor authentication' as an attempt to describe the applicable security measure without appropriate elaboration of how, where, to whom, and when the measure applies would not address the requirement. Instead, 'password security is managed through complexity requirements involving a minimum of 10 characters comprising letters, numbers and symbols and a requirement to change passwords every 90 days' for example, would be more appropriate.

OFFICIAL



Australian Government  
Department of Home Affairs

# Transport Security Reform: Legislative Package

## Critical systems

Cohort	Example of a critical system
Aviation	
Aviation security	<ul style="list-style-type: none"><li>regulated agent and/or known consignor databases</li><li>access control and alarm monitoring systems</li><li>closed-circuit television (CCTV) surveillance systems</li><li>passenger and baggage reconciliation systems</li><li>screening systems and/or explosive detection systems, whether networked or operating in a stand-alone configuration</li></ul>
Aviation safety	<ul style="list-style-type: none"><li>air traffic management systems</li><li>departure control systems</li><li>communication, navigation, and other safety-critical systems of an aircraft</li><li>aircraft command, control, and dispatch systems</li></ul>
Aviation facilitation	<ul style="list-style-type: none"><li>aircraft operator reservation and passenger check-in systems</li><li>flight information display systems</li><li>baggage handling and monitoring systems</li><li>border crossing and customs systems</li></ul>
Maritime	
Port	<ul style="list-style-type: none"><li>configuration, identification, and use of control systems</li><li>critical permanent plant or machinery</li><li>security or other control rooms, including guarding</li><li>security, alarm and access control systems, CCTV, and video processing</li><li>reliance on GNSS technology for port operations</li><li>cabling routes and their containment (for example, ducts and trunking)</li><li>detection systems, whether networked or operating in a stand-alone configuration</li><li>terminal operating systems</li><li>operational technology</li></ul>
Ship	<ul style="list-style-type: none"><li>cargo management systems</li><li>bridge systems</li><li>propulsion and machinery management and power control systems</li><li>access control systems</li><li>passenger servicing and management systems</li><li>passenger facing public networks</li><li>administrative and crew welfare systems</li><li>communication systems</li><li>navigation systems</li><li>operational technology</li></ul>
Offshore facilities	<ul style="list-style-type: none"><li>drilling control systems</li><li>passenger control systems</li><li>vessel management systems</li><li>dynamic positioning systems</li><li>stability analysis systems</li><li>weight control systems</li><li>operational technology</li></ul>

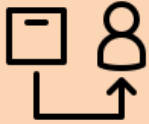
The information contained in this document is general in nature and does not constitute legal advice. Industry participants are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.



## Transport Security Reform: Legislative Package

### Resilient to current and emerging threats

#### Supply chain security



##### Obligations to be specified in the Regulations

- Identify supply chain hazards that could significantly interfere with the IP or its operations.
- 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.
- 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
  - the vulnerability of using one provider
  - any failure or lowered capacity of other assets in the IP's supply chain.

#### What constitutes your supply chain?

The extent of your entity's supply chain will be contextual. You should consider the key service providers required to operate your critical asset or deliver goods and services.

#### What constitutes a major supplier?

Entities need to consider whether their SP lists major suppliers; specified as 'any vendor that by nature of the product or service they offer, has a significant influence over the security of a responsible entity's critical asset'.

These suppliers must be identified in the body of your SP rather than within your security assessment.

There will be **no prescriptive definition** of 'supply chain' in the transport security legislative frameworks.

#### Security risks relevant to your supply chain

This will require you to identify the hazards or harm arising from threats to people, assets, equipment, products, services distribution, and intellectual property within supply chains, and what you are doing to mitigate these.

This requirement may be met by describing:

- an overview of the processes and controls used to identify supply chain risks
- the risks identified
- the controls or strategies to mitigate these risks.

The department will host workshops on your supply chain security obligations to assist with implementation.

#### Mitigation measures may include:

- ensuring major suppliers with access to sensitive data have sufficient security personnel and cyber security resilience policies built into contract arrangements
- identifying and reducing dependencies and supply chain bottlenecks through diversification of vendors
- establishing within contracts financial viability assessments, proof of relevant insurance coverage, due diligence reviews including risk ratings and findings, vendor security assessments including a technical assessment of their cyber security posture, and privacy impact assessments prior to procurement
- establishing data retention and destruction provisions in supplier agreements following the cessation of services
- establishing clear responsibilities between supplier and customer, should a data breach occur, including allocating who should assess and notify the breach.



## Resilient to current and emerging threats

### Natural hazards



#### Obligations to be specified in the Regulations

Outline processes to minimise risks arising from natural hazards on your entity, and mitigate against its physical impacts and effects.

#### Scope of natural disasters

Natural disasters have the potential to cause widespread impacts, losses, and damages, including potential damage to infrastructure. The unpredictability and unprecedented nature of these events can impact the security and stability of critical assets.

Under this measure, you will need to consider types of extreme weather events (such as floods or bushfires) rather than individual weather events such as the 2019-20 bushfires, or the 2011 Brisbane floods. Entities must consider each relevant hazard to the geography of your operations, and have in place procedures to deal with their potential materialisation.

#### For example

- ✓ An SP that considers the consequences of, and articulates mitigations for, floods holistically in regards to its operations.
- ✗ An SP that considers the consequences of, and articulates mitigations for bushfires or floods in regard to its aircraft in flight over a specific region only.

#### Mitigation measures may include:

Depending on your entity's operating environment and geography, mitigation methods may include:

- fostering infrastructure resilience and preparedness through contingency planning, emergency exercises, and simulations to ensure staff are prepared to act in case of emergency
- developing and maintaining a bushfire survival plan which could include controlled burning of surrounding forestry, or the installation of bushfire sprinklers to reduce the likelihood and consequences of a potential fire
- de-clustering of key assets for example, spreading infrastructure across multiple sites and maintaining backup infrastructure in peak hazard periods to increase resilience and ensure a single hazard cannot disable a majority of your assets
- establishing plans and process to maintain operations where possible in the case of a natural hazard to support emergency services, communities, and recovery operations
- pre-establishing manual operating procedures or perimeter security procedures to be deployed in the circumstance where a natural hazard may degrade your standard operations or boundaries.

We will work with you to identify where existing documents (such as a business continuity plan or emergency management plan) can satisfy these regulatory requirements.



**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 4**

**Subject: Powers given to the Secretary of Home Affairs to impose additional security measures**

***Asked by:*** Raff Ciccone

***Question:***

The Special Security Direction provisions give the Secretary of the Department of Home Affairs powers to impose additional security measures in certain circumstances—why has this been deemed necessary?

***Answer:***

The Secretary of the Department of Home Affairs already has the power to issue a special security direction (under the Aviation Transport Security Act 2004 (ATSA)), or a security direction (under the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) (collectively SSDs)), but only in limited circumstances:

- under ATSA, where a specific threat of unlawful interference exists; or there is a change in the nature of an existing general threat of unlawful interference; or a national emergency declaration (within the meaning of the National Emergency Declaration Act 2020) is in force and the Secretary is satisfied that additional security measures are appropriate to support the national emergency declaration.
- under MTOFSA, where an unlawful interference with maritime transport or offshore facilities is probable or imminent or a national emergency declaration (within the meaning of the National Emergency Declaration Act 2020) is in force and the Secretary is satisfied that the security direction is appropriate to support the national emergency declaration.

This Bill expands the types of circumstances where an SSD might be considered, in response to a significant threat in line with the expanded scope of the ATSA and MTOFSA outlined in the Explanatory Memorandum.

SSDs are considered a measure of last resort, where existing measures are deemed insufficient to mitigate a particular risk or change in the threat environment. SSDs have never been used in the maritime sector, and on only four occasions for the aviation sector. When they have been used, they have been necessary, and effective, in mitigating risks until the threat was resolved or a longer term regulatory solution was implemented.

- In 2006, an SSD was issued requiring aviation industry participants to implement immediate restrictions on the amount of liquids, aerosols and gels that could be taken as carry-on luggage on board an aircraft. The SSD was made to align with international action undertaken in response to a security event until a longer-term solution could be implemented in regulations.
- In 2017, in response to a terrorist plot at Sydney Airport:
  - an SSD was issued requiring additional passenger security screening measures until the security situation was resolved; and
  - at a later stage, a second SSD was issued requiring aviation industry participants (IPs) to implement immediate restrictions on the amount of inorganic powder that could be taken as carry-on luggage on board an aircraft. The SSD was made so that a longer-term solution could be implemented in regulations.
- In 2024, in response to a global air cargo supply chain threat, an SSD was issued to IPs requiring additional security measures be implemented for cargo coming in to Australia.

SSDs are designed with in-built review and sunset mechanisms to ensure government addresses the issue through a long-term solution, such as regulation change, if needed. Under the ATSA and MTOFSA, an SSD remains valid for three months and must be revoked once the specific or general threat no longer exists. Under the ATSA, the Secretary has the power to extend the SSD for a further three months following mandatory industry consultation and a written notice. The ATSA specifically notes that once an SSD has been in force for six months, the Secretary cannot issue the same or a similar SSD for a period of six months.

Extending the scope of SSDs, and creating consistency between the ATSA and MTOFSA, will ensure that the existing last resort power is available across the additional security circumstances needed to secure critical aviation and maritime infrastructure.

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 5**

**Subject: Streamlining Commonwealth reporting**

***Asked by:*** Raff Ciccone

***Question:***

Industry stakeholders have identified several Commonwealth agencies they must already report to including the Civil Aviation Safety Authority, Australian Transport Safety Bureau and Bureau of Meteorology. The Bill requires further reporting to both Home Affairs and the Australian Signals Directorate. What is being done to streamline reporting to the Commonwealth?

***Answer:***

The department is very aware that aviation and maritime industry participants are also regulated under other, non-security legislation. In developing the Bill, the department considered other regulatory frameworks and where there may be possible touch points.

The all hazards security obligations have been designed to complement, not duplicate, existing regulations, where appropriate. Consultation with industry and relevant government agencies in the development of the regulations will ensure any duplication across any other relevant legislative frameworks is identified and resolved.

**Cyber reporting**

The Department is working across the Government to streamline cyber security incident reporting and reduce duplicative reporting requirements for regulated entities, as part of Horizon 1 of the 2023-2030 Australian Cyber Security Strategy. Currently, the Department is working with stakeholders to explore non legislative, low or no cost technological enhancements to the current single reporting portal on [cyber.gov.au](https://cyber.gov.au). The Department is also looking at structural reform options for future harmonisation of cyber regulations and will be working with regulators to simplify their reporting forms. The Department will continue to work closely across Government and with industry to streamline cyber security incident reporting. Cyber security incident reporting obligations under the Aviation Transport Security Act 2004 (ATSA) and the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) will be included within this project.

### ***Civil Aviation Act 1988***

The *Civil Aviation Act 1988* prohibits conduct which would affect aviation safety, whereas this Bill imposes positive obligations to actively mitigate against all hazards security risks. There appears to be no duplication between this Act and the Bill.

The *Civil Aviation Safety Regulations 1988* (CASR) establishes a scheme for safety management systems and risk management plans. The scope of these is limited to safety risks which operators are exposed as a consequence of specific hazards attributed to their operation. It is separate to the security risks which must be considered under this Bill.

The Civil Aviation Safety Authority administers Aerodrome Emergency Plans under CASR Part 139/Manual of Standards Part 139 (AEP). This circular advisory is only applicable to aerodrome operators, and does not cover the breadth of the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (TSA) Bill within the aviation sector. The AEP circular advisory requires the pre-planning of response measures to be enacted in the circumstance of a natural disaster. This does not duplicate the proposed natural hazards security obligations within the TSA Bill, which focus uniquely on the pro-active mitigation of natural hazards risks on security operations.

### ***Transport Safety Investigation Act 2003***

The *Transport Safety Investigation Act 2003* includes reporting requirements for immediate, and routinely, reportable matters. The voluntary reporting requirements in this Act explicitly exclude the reporting of criminal conduct, being terrorist acts, and acts of unlawful interference. There appears to be no duplicative reporting obligations between this Act and the Bill.

### ***Navigation Act 2012 and Marine Safety (Domestic Commercial Vessel) National Law Act 2012***

The *Navigation Act 2012* and the *Marine Safety National Law Act 2012* both include incident reporting requirements for safety incidents. Such incidents specifically include those resulting in the death of a person, serious injury to a person, loss of a vessel, loss of a person from the vessel, or significant damage to the vessel. There appears to be no duplicative reporting obligations between either of these Acts and the Bill.

### ***Australian Maritime Safety Authority Act 1990***

The *Australian Maritime Safety Authority Act 1990* includes positive obligations on entities to take reasonable care for safety. There appears to be no duplication between the safety risks considered by this Act, and the all hazards security obligations in this Bill.

### **State and Territory legislation**

Initial research reveals that state and territory legislation which crosses over with the Bill for aviation and maritime entities tend to be in the context of emergency management, rather than all hazards security risks.

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 6**

**Subject: Obligations in the Bill and obligations in the SOCI Act**

**Asked by:** Raff Ciccone

**Question:**

How do the new obligations in the Bill sit alongside the obligations in the Security of Critical Infrastructure Act?

**Answer:**

The obligations in the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (TSA) Bill will complement those in the *Security of Critical Infrastructure Act 2018* (SOCI Act).

Under the SOCI Act, critical infrastructure assets are required to identify, prevent, and mitigate material risks from all hazards in a Critical Infrastructure Risk Management Program (CIRMP). Currently, critical aviation assets and critical ports are not required to have a CIRMP; instead these assets would be required to comply with all hazard security obligations under the transport security legislative frameworks.

It is the department's intent that, where industry participants may be captured by other obligations under both SOCI and the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003* (the transport security legislative frameworks), their obligations will be fulfilled through the transport security legislative frameworks, and any duplication with the SOCI Act will be avoided. The Department will undertake further work to ensure this can be achieved.

For instance, both the transport security legislative frameworks and the SOCI Act require mandatory reporting of cyber security incidents if the incident has a relevant, or significant, impact. These obligations currently apply to critical aviation assets and critical ports under the SOCI Act. When the cyber incident reporting obligations come into effect under the transport security legislative frameworks, the Department's intent is that these entities would only need to report under the transport security legislative framework. The department intends to make amendments to legislative instruments related to the SOCI Act to facilitate this.

Currently, under the transport security legislative frameworks, industry participants are required to implement measures and procedures that mitigate risks associated with physical and personnel

security threats within their security programs or plans. Under this Bill, 'all hazard security risks' is a collective term that comprises physical, personnel, cyber, supply chain, and natural hazard risks. Under the Bill, certain industry participants will be required to proactively identify, mitigate, and manage all hazard security risks that may impact its business operations. These obligations have been modelled on the obligations within the CIRMP under the SOCI Act, where possible.

The below table outlines the similarities between the all hazards security obligations under this Bill and those within the CIRMP under the SOCI Act. Please see the answer to question 7 for details on which entities are subject to each obligation across the proposed framework.

All hazards domain	Proposed additional regulatory obligations under the Bill	Equivalent obligations in the SOCI Act
Personnel security	<ul style="list-style-type: none"> <li>Under the proposed regulations, industry participants will be required to identify and mitigate risk associated with personnel who have access to, or influence over, security areas, or critical systems, remotely</li> <li>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.</li> </ul>	No
Cyber security	<ul style="list-style-type: none"> <li>Minimise cyber security risks, and mitigate their impact by complying with the most recent edition of one, or a combination of multiple, established cyber security frameworks</li> <li>Establish processes to protect critical systems and data.</li> </ul>	Yes
Supply chain security	<ul style="list-style-type: none"> <li>Identify supply chain hazards that could significantly impact the IP or its operations</li> <li>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 and</li> <li>Minimise or eliminate risks 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.</li> </ul>	Yes
Natural hazards	<ul style="list-style-type: none"> <li>Outline processes to minimise risks arising from natural hazards on the regulated IP, and mitigate against its physical impacts and effects.</li> </ul>	Yes

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 7**

**Subject: Current obligations under the SOCI Act and potential changes**

**Asked by:** Raff Ciccone

**Question:**

What obligations do the aviation and maritime industries currently have under the Security of Critical Infrastructure Act, and how will these change with the Bill?

**Answer:**

The industry participants captured under the *Security of Critical Infrastructure Act 2018* (SOCI Act) are a subset of the industry participants that are regulated under the transport security legislative frameworks.

The SOCI Act captures critical aviation assets and critical ports, which are already regulated under the *Aviation Transport Security Act 2002*, and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) (the transport security legislative frameworks). There is also a small cohort of unique industry participants operating 'critical data storage and processing assets', 'critical electricity assets', 'critical freight services assets', 'critical gas assets', 'critical liquid fuel assets', and 'critical liquid fuel storage assets' which are also regulated under both the SOCI Act and the MTOFSA.

Critical aviation assets and critical ports are not subject to obligations to maintain a critical infrastructure risk management plan (CIRMP) under the SOCI Act.

By introducing the obligations into the transport security legislative frameworks, the significant breadth and diversity of the transport sector is captured, elevating the security of the transport sector holistically.

Noting the SOCI Act also contains mandatory cyber incident reporting requirements, the department will work on solutions to ensure there is no unnecessary duplicative obligations requiring entities captured under the SOCI Act to report the same incident under two legislative frameworks.

There remains a small cohort of entities who are captured as critical infrastructure assets under SOCI and regulated under MTOFSA who are currently expected to maintain a CIRMP as part of their SOCI obligations. The Department will work with these entities to explore possible options to reduce or remove regulatory duplication as necessary, including the possibility of removing their requirement to comply with certain SOCI obligations.

For completeness, the Department notes that, through this Bill, the definition of a 'security regulated port' is proposed to be extended through the Bill to clarify a port also includes anything else that is critical to ensuring the security and reliability of the ports defined functions (e.g. where goods are loaded to land-based transport from a *ship*). This will have flow on impact to those critical ports regulated under the SOCI Act, which relies on the definition of 'security regulated port' under the MTOFSA. The extended definition largely clarifies the existing definition and is not expected to broaden existing obligations under the MTOFSA.



**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 8**

**Subject: Increase to regulatory workload**

**Asked by:** Raff Ciccone

**Question:**

The Bill intends to widen the scope of matters to be reported to Home Affairs, which will increase its workload as the relevant regulator, what consideration has been given to increasing the capacity of the Department to manage this increased workload?

**Answer:**

The department acknowledges the Bill will increase the workload of the Regulator and is refining its regulatory position statement; compliance and enforcement policy framework; and regulatory priorities to effectively direct regulatory and policy resources to key areas of focus and risk. These initiatives will help to ensure there is risk-based targeted effort and investment across high priority areas, or areas of significant concern.

In line with the department's additional estimates statements 2024-25, transport security has been funded \$146,435 million for departmental expenses over the forward estimates. Please see the below table for a breakdown of the costs per financial year.

2024-25 (Budget)	2025-26 (Forward estimate)	2026-27 (Forward estimate)	2027-28 (Forward estimate)
36,438 million	36,274 million	36,807 million	36,916 million

**HOME AFFAIRS PORTFOLIO  
DEPARTMENT OF HOME AFFAIRS**

**PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE**

Parliamentary Joint Committee on Intelligence and Security

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

20 February 2025

**QoN Number: 9**

**Subject: Provisions for the current penalty regimes**

**Asked by:** Raff Ciccone

**Question:**

Please detail how the current penalty regimes are provided for in the Aviation Transport Security Act 2004 and Maritime Transport and Offshore Facilities Security Act 2003. Are these arrangements considered unusual within Commonwealth law and has consideration been given to the merits of altering these arrangements?

**Answer:**

The penalty regimes exist within the transport security legislative frameworks – both acts and regulations, and largely align with the principles set out in the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide).

As per 3.1.1 of the Guide, the penalties in the Aviation Transport Security Act 2004 (ATSA) and the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) are designed to deter the commission of offences, and reflect the severity of the violation within the legislative schemes. ATSA and MTOFSA are critical schemes impacting the lives of millions of passengers annually. As such, the industry participants responsible for ensuring the safety and security of these individuals is responsible for a higher standard of procedures, with corresponding penalties for non-compliance.

The *Civil Aviation Act 1988* and the *Civil Aviation Regulations 1988* follow a similar approach to ATSA and MTOFSA where offences and corresponding penalty units are placed in the both the Act and Regulations.

The proposed penalty for a failure to report a cyber-security incident aligns with the penalties for failure to report other kinds of security incidents as provided for within the transport security legal frameworks – the Aviation Transport Security Act 2004 (ATSA) and its regulations, and the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) and its regulations.

The intention in aligning the strict liability penalties in this way is to maintain consistency across the legislation and reinforce the importance of reporting in responding to or mitigating acts of unlawful interference. This also recognises the significance of cyber security incidents, alongside other more conventional threat types (like personnel or physical threats). A malicious cyber incident could have a significant adverse impact, not just on the operations of aviation and maritime industry participants, but also through cascading effects to any dependent infrastructure, networks, and the Australian

public more broadly. As such, it is imperative that timely reporting of such incidents is properly mandated and enforceable.

An increase in the number of penalty units for offences under the ATSA or MTOFSA could act as a more significant deterrent to non-compliance, and incentivise industry to achieve better security outcomes. Any changes to the penalties would need to be in line with the *Regulatory Powers Act 2014*, the Guide, and any other relevant legislation.