December 2021

Guide to the exposure draft Transport Security Amendment (Critical Infrastructure) Bill 2022

Contents

Introduction

The Government is progressing reforms to uplift the security of 11 sectors critical to the economic and social wellbeing of the nation, or to Australia's national security and defence including the aviation and maritime transport sectors. These reforms will support industry to better mitigate against, and respond to, the dynamic and rapidly evolving range of threats existing today and into the future.

The reforms are primarily being progressed through amendments to the *Security of Critical Infrastructure Act 2018* (SoCI Act). The Security Legislation Amendment (Critical Infrastructure) Bill 2021 (SLACI Bill One), which passed Parliament on 22 November 2021, and a planned second Bill (SLACI Bill Two) are being progressed to make these changes following recommendations from the Parliamentary Joint Committee on Intelligence and Security to split the SLACI Bill into two separate Bills.

To reflect the mature regulatory framework already in place for the aviation and maritime transport sectors, dedicated reforms are being developed to meet the intent of the critical infrastructure reforms. The aviation and maritime critical infrastructure reforms will amend the *Aviation Transport Security Act 2004* (Aviation Act) and the *Maritime Transport and Offshore Facilities Security Act 2003* (Maritime Act), collectively the Acts. These amendments, captured in the Transport Security Amendment (Critical Infrastructure) Bill 2022 (Transport Security Bill), are the most significant reforms to the Acts since their creation and will uplift the Acts from a focus on unlawful interference to encompass an **all hazards** risk management framework.

This Guide has been developed to provide further information on key amendments proposed in the Transport Security Bill and should be read alongside the Transport Security Bill exposure draft.

Key Amendments

The Transport Security Bill will:

- Amend the definition of **unlawful interference** to explicitly include **cyber security incidents.**
    - This will apply to all regulated aviation industry participants[1] and regulated maritime industry participants[2].
- Introduce a new purpose, into both Acts, of safeguarding against **operational interference** which will capture all hazards beyond those already captured under unlawful interference.
- Introduce powers for the Minister for Home Affairs (the Minister) to declare select industry participants as **'critical industry participants**'.
    - Critical industry participants will be required to identify, and mitigate against, acts of unlawful interference and operational interference.
    - Only a small group of regulated industry participants will be declared critical.
- Amend security plans and programs, to include a **security assessment** to be undertaken as part of a plan or program for aviation industry participants. This will bring the two Acts into alignment.
- Modernise compliance powers for aviation and maritime security inspectors, including triggering Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014*.

[1] An aviation industry participant means: an airport operator; an aircraft operator; a known consignor; a regulated agent; a person who occupies or controls an area of an airport; a person appointed by the Secretary to perform a security function; Airservices Australia; a contractor who provides services to a person mentioned – Section 9 Aviation Act

2 A maritime industry participant means: a port operator; a port facility operator; the ship operator for a regulated Australian ship; the ship operator for a regulated foreign ship; an offshore industry participant; a contractor who provides services to a person mentioned; a person who conducts a maritime-related enterprise – Section 10 Maritime Act

- Amend a number of existing requirements under the Acts to encompass the new purpose of operational interference.

The Transport Security Bill has two Schedules, each containing two Parts.

- **Schedule 1: Aviation Act**
    - Part 1 – Contains general amendments to the Aviation Act.
        - Including amendments to unlawful interference, improvement notices and additional compliance powers.
        - Amendments to reflect the commencement of the *Federal Circuit and Family Court of Australia Act 2021*.
    - Part 2 – Contains amendments to the Aviation Act to include operational interference.
- **Schedule 2: Maritime Act**
    - Part 1 – Contains general amendments to the Maritime Act.
        - Including amendments to unlawful interference, improvement notices and additional compliance powers).
        - Amendments to reflect the commencement of the *Federal Circuit and Family Court of Australia Act 2021*.
    - Part 2 – Contains amendments to the Maritime Act to include operational interference.

References for key amendments have been provided in the text of the Guide. A full list of references within the Transport Security Bill can be found at **Attachment B**.

1. Definitions

1.1. Unlawful interference changes

Under the Acts, **unlawful interference** safeguards against something done without lawful authority that interferes with the security of passengers, goods and infrastructure.

The Transport Security Bill will expand the definition of unlawful interference to explicitly include **cyber security incidents** and to capture additional trusted insider threats. The proposed amendments will remove the requirement that information being communicated needs to be 'false' (Maritime Act Section 11(1)(h)) or 'false or misleading' (Aviation Act Section 10(1)(g)) to be an act of unlawful interference. This will support capturing cyber security and trusted insider threats when an action taken may be done without lawful authority but is not false or misleading. Information that is communicated lawfully and in good faith is not an act of unlawful interference.

These amendments can be found at:

- For the Aviation Act: Schedule 1 (Part 1) – Item 52
- For the Maritime Act: Schedule 2 (Part 1) – Item 12

Cyber security incident

A new definition of a **'cyber security incident'** will be introduced reflecting the changing security environment. Cyber security incidents that have a **'relevant impact'** will need to be reported to the Department and the Australian Signals Directorate. Further detail on thresholds will be provided in the

Aviation Transport Security (Incident Reporting) Instrument 2018 and the Maritime Transport and Offshore Facilities Security (Incident Reporting) Instrument 2018, collectively the Incident Instruments, and guidance. It is anticipated that these will be identical to what is in SLACI Bill One.

Due to the sequencing of legislative changes, the Department has recommended to Government that mandatory cyber incident reporting obligations are activated through SLACI Bill One to ensure these sectors are covered by these requirements.

If Parliament passes the Transport Security Bill, these obligations could be activated through the Aviation and Maritime Acts at which time the obligation under the SoCI Act could be 'turned off'.

There is no intention to create duplicative obligations requiring entities to report the same incident under two legislative frameworks. Government will consult with industry on the best approach to ensure the intent is met without creating undue regulatory burden.

1.2. Operational interference

A new definition of **'operational interference'** would be inserted into both Acts

Under 'operational interference' a smaller group of industry participants will be required to identify and take reasonable steps to mitigate against all forms of interference that could impact the **confidentiality availability, integrity, and/or reliability** of their operations and assets. This will capture both human-induced and natural hazards that could impact an industry participant's business, such as personnel threats or supply chain security.

Further detail and thresholds to support operational interference will be included in associated changes to the *Aviation Transport Security Regulations 2005* (Aviation Regulations) and the *Maritime Transport and Offshore Facilities Security Regulations 2003* (Maritime Regulations) collectively the Regulations, which will undergo co-design with industry.

If a hazard meets the threshold of both unlawful interference and operational interference, the hazard will **only** be considered unlawful interference. As with the current definition of unlawful interference, operational interference will not include lawful protest, advocacy, dissent or industrial action.

The Secretary of the Department (the Secretary) will be able to use a number of existing powers to safeguard against operational interference, in line with similar requirements to safeguard against unlawful interference, including:

- prescribing areas and security zones for airports, ports and offshore facilities;
- prescribing measures for on board security in the Maritime Act;
- prescribing types of information that is considered 'aviation security information' in the Aviation Act; and
- enforcement orders.

These can be found at:

- For the Aviation Act: Schedule 1 (Part 2) – Item 75
- For the Maritime Act: Schedule 2 (Part 2) – Item 117

1.3. Critical industry participant

The Transport Security Bill will introduce a power for the Minister to declare certain industry participants as 'critical'. In doing so, the Minister must consider the impact on Australia's social and economic wellbeing,

national security and defence if an industry participant is unable to operate. This will support continued alignment with the SoCI Act and the creation of a cohesive critical infrastructure framework.

Further detail on the criteria and thresholds that will guide a Ministerial declaration will be developed in consultation with industry. It is intended that the classification of an industry participant as 'critical' will be a point in time declaration, not one that industry participants will enter and exit as their business changes (as is the case under the current airport tiering system). The Department will consult with individual industry participants to seek their views before they are declared critical by the Minister.

These amendments can be found at:

- For the Aviation Act: Schedule 1 (Part 2) – Item 76
- For the Maritime Act: Schedule 2 (Part 2) – Item 118

2. Security program changes

Amendments to security program[3] requirements will be made in the Regulations using existing powers in the Acts to align with the Critical Infrastructure Risk Management Program (RMP) obligations proposed within SLACI Bill Two. Aviation and maritime industry participants will not be required to complete a RMP under the SoCI Act, as the amended security program obligations will fulfil this requirement using the existing processes under the Aviation and Maritime Acts.

The new requirements of security programs will be settled in consultation with industry during the regulatory co-design process.

2.1. Security assessments

New powers will be introduced into the Aviation Act, through the Transport Security Bill, requiring industry participants to undertake a **security assessment** (to include a risk assessment) on the hazards that will impact their operations. The security assessment will inform the contents of the security program, replacing the risk context statement for aviation.

The Transport Security Bill may require air cargo agents to complete a security assessment, depending on their classification and criticality. The intent is that:

- Regulated air cargo agents will be required to complete a security assessment.
- Accredited air cargo agents and known consigners will not be required to complete a security assessment.

Government will consult with industry on the best approach to ensure the intent is met without creating undue regulatory burden.

The existing Secretary's Determination for cargo examination will be amended so that it may also prescribe training requirements for aircraft operators who examine cargo. This is to correct an oversight in the Aviation Act.

These amendments can be found at:

- For the Aviation Act: Schedule 1 (Part 1) – Item 18
- For the Maritime Act: Schedule 2 (Part 1) – Item 24

[3] Each sector has a different name for their security program: transport security programs (aviation); security programs (air cargo); maritime security plan (port operators and port facility operators); ship security plan and offshore security plan. Security programs are similar in form across sectors, with the content being specific to the operating environment of each industry participant.

2.2. Secretary given security programs

Under the Aviation Act, the Secretary may issue a security program to an aviation industry participant. These programs allow the Department to provide a 'model' security program to lower risk industry participants.

This provision will be inserted into the Maritime Act to align it with the Aviation Act. This will ensure that the Secretary may, if required, issue a security program to an industry participant that will set out measures that include safeguarding against unlawful interference and operational interference.

The **Secretary given security programs** are intended to be used to provide a baseline cyber security framework, to reduce the regulatory obligation on lower risk industry participants.

The decision to issue a security program will be reviewable by the Administrative Appeals Tribunal.

A Secretary given security program can be held by an industry participant in addition to their custom security program.

These amendments can be found at:

- For the Maritime Act: Schedule 2 (Part 2) – Items 123, 126, 129

2.3. Consideration periods

The Transport Security Bill will repeal, across both Acts, the mandated (45 day) timeframe under which an industry participant must provide further information as requested by the Secretary during the regulatory assessment process.

Instead, an appropriate time will be set by a written notice for industry to respond to the request for further information. An industry participant may request an extension to this timeframe. The consideration period will recommence with a 30 day period once the requested information is received by the Secretary.

These amendments aim to improve clarity and reduce the regulatory burden on industry participants. The existing requirement provides limited flexibility for an industry participant to fulfil complex requests for information from the Secretary within the statutory timeframe.

This change will impact the decision to approve a security program, to approve the alteration of a security program or to approve the cancellation of a security program. It will also extend the power to request further information, without timeframe, when an industry participant requests to alter their security program.

- For the Aviation Act: Schedule 1 (Part 1) – Items 19-22.
- For the Maritime Act: Schedule 2 (Part 1) – Items 25-29, 36-39 and 46-49.

3. Periodic reporting

The Transport Security Bill will introduce a requirement for industry participants to provide a **periodic report** to the Secretary on their security program.

3.1. Who needs to submit a report?

All industry participants who are required to give the Secretary a security program will be required to submit a periodic report. The timing and content of the report will be based on whether an industry participant is considered 'critical'.

- Critical industry participants will be required to submit a report annually aligning with similar provisions to be proposed in SLACI Bill Two.
- Other industry participants will be required to submit a report 30 months from the commencement of their security program. This reflects the average approval period of 60 months for a security program and is intended to ensure that industry participants provide a periodic report halfway through the life of the security program.

The requirement to submit a periodic report will not apply to industry participants with Secretary given programs.

An industry participant may be required to submit an ad hoc report to the Secretary in relation to their security program upon request or direction. This would be used to capture those industry participants who have security programs approved for a period different from the standard five years.

These amendments can be found at:

- For the Aviation Act: Schedule 1 (Part 1) – Item 47 & Schedule 1 (Part 2) – Item 89
- For the Maritime Act: Schedule 2 (Part 1) – Item 90 & Schedule 2 (Part 2) – Item 136

3.2. Content of the report

The periodic report will require an industry participant to provide:

- a statement about whether their security program is up to date; and
- whether the security program adequately addresses their statutory requirements in relation to aviation or maritime security.

The Regulations, to be co-designed with industry, will further prescribe what matters are to be included in these reports, to be co-designed with industry. The intent is to include an obligation that the outcomes of any internal reviews or audits conducted within the reporting period are included within the report.

Civil penalties for failing to submit a report within the specified timeframe will apply to industry participants required to make a periodic report, consistent with the obligations to be proposed within SLACI Bill Two.

4. Compliance powers

The powers of aviation and maritime security inspectors will be modernised to enable compliance activities to be undertaken against the new obligations within the Transport Security Bill. The proposed amendments will also ensure greater alignment of powers between the Acts and with other Australian Government regulatory frameworks.

4.1. Notices and system testing

The Transport Security Bill will introduce powers allowing aviation and maritime security inspectors to issue a written notice to:

- Require an industry participant or one of their employees to provide specific assistance.
- Require an industry participant to provide information where the inspector believes the information would be reasonably necessary to exercise their powers.

The Transport Security Bill will also amend:

- Existing powers that allow an inspector to operate equipment for the purpose of gaining access to documents or records.
- Existing notices on the provision of security compliance information to include the provision of information the industry participant can obtain, not only information that the industry participant 'has'.
- The power to operate and connect a device to equipment at a location operated by an aviation or maritime industry participant for the purpose of testing the equipment.

4.1.1. Improvement notices

The Transport Security Bill introduces powers allowing aviation and maritime security inspectors to issue improvement notices to industry participants. The improvement notice framework proposed is based on the framework within the *Work, Health and Safety Act 2011.*

If issued, an improvement notice will require an industry participant to take actions to rectify or prevent a contravention. Failure to comply with an improvement notice will attract civil penalties against a person or corporation associated with the improvement notice. The issuing of improvement notices can be subject to internal review, with the ability to appeal to the Administrative Appeals Tribunal.

4.1.2. *Regulatory Powers (Standard Provisions) Act 2014*

The Transport Security Bill will trigger Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), which deals with investigation powers for Australian Government agencies. This will also modernise the regulatory framework and align it with other Australian Government frameworks.

These powers will enable an aviation or maritime security inspector to be supported by an **appropriately qualified specialist assistant** in the course of their duties. The specialist assistant will not have independent action powers but will be able to exercise the powers of the inspector that is supervising them. This will allow aviation and maritime security inspectors to confirm compliance with parts of the Acts that they might not have sufficient expertise in, for example cyber security.

These powers will also grant aviation and maritime security inspectors **investigation powers** in instances where the inspector suspects on **reasonable grounds** that there may be material on the premises that relates to a contravention of the Acts. They will be able to search places of operations of industry participants, ask persons on the premises questions, bring equipment on to the premises, operate equipment, and (with a warrant) collect and record evidence.

4.1.3. Maritime systems testing

New powers for **security systems testing** will be inserted in the Maritime Act to mirror the amendments made to the Aviation Act by the *Transport Security Amendment (Testing and Training) Act 2020*. This will grant maritime security inspectors the power to test a security system, including by using a test weapon.

5. Information sharing

The Transport Security Bill will introduce provisions on the **use and disclosure of protected information** across both Acts. This is to ensure that information provided under the Acts are protected by a more robust framework that outlines the limited circumstance when it can be shared. Protected information will include information obtained by a person performing their duties, security compliance information, aviation security information and the contents of a security program.

The following types of authorised uses and disclosures of protected information will be provided for:

- disclosing information in the course of exercising a power, performing a function or duty under both Acts, or ensuring compliance with both Acts;

- the Secretary disclosing to identified Australian Government Ministers, their staff, or an agency they administer that is responsible for functions appropriate to why the information was collected;
- the Secretary disclosing to state and territory government ministers, their staff, or an agency that they administer that is responsible for functions appropriate to why the information was collected;
- the Secretary disclosing to an enforcement body for an enforcement related activity;
- a person using or disclosing the information for the purpose that it was disclosed to them; and
- disclosures to a person specified by the Secretary in a legislative instrument. This type of disclosure will have appropriate record keeping requirements.

This will establish a framework to protect information that is held by both industry and the Department.

6. Additional changes

6.1. Security directions

The Transport Security Bill will make amendments to the Secretary's existing powers to give special security directions (Aviation Act) and security directions (Maritime Act). These changes update these powers to address the expanded scope of unlawful interference and the new purpose of operational interference.

Additional amendments to the Maritime Act will give the Secretary the power to give a direction in relation to a specific threat of unlawful interference, a change in the general threat of unlawful interference, and in relation to a national emergency declaration (within the meaning of the *National Emergency Declaration Act 2020*). This will align the power in the Maritime Act with the Aviation Act.

6.2. Delegations

The Transport Security Bill will make amendments to both Acts to expand the ability of the Secretary to delegate their powers to the head of another agency. Under the amendments, agency heads must agree to the delegation in writing.

The amendments would remove the restriction that the Secretary can only delegate to other agencies whose functions relate to national security. This reflects the proposed broader remit of both Acts.

Attachment A – Glossary

Term	Definition
All hazards	Human induced hazards, or natural events that could present a risk to the operation and security of an industry participant. The term is used to capture the broader remit of operational interference, as opposed to the hazards already captured under unlawful interference.
Aviation and maritime security inspectors	Employees of the Department of Home Affairs, or certain law enforcement officers, who are appointed to undertake compliance activities under the Aviation and Maritime Acts.
Aviation Transport Security Act 2004 **(Aviation Act)**	The Act of Parliament responsible for the regulation of the security of airports, airlines and air cargo agents.
Aviation Transport Security Regulations 2005 **(Aviation Regulations)**	Supporting regulations to the Aviation Act which provides more detail on the regulatory framework.
Critical industry participant	A limited subset of aviation and maritime industry participants that are declared as critical to Australia's social and economic wellbeing, national security and defence by the Minister for Home Affairs
Critical Infrastructure Risk Management Program (CIRMP)	A proposed amendment in SLACI Bill Two requiring the responsible entities of critical assets to provide information on how they are meeting the requirements of the SoCI Act.
Maritime Transport and Offshore Facilities Security Act 2003 **(Maritime Act)**	The Act of Parliament responsible for the regulation of the security of ports, port facility operators, registered ships and offshore oil and gas facilities.
Maritime Transport and Offshore Facilities Security Regulations 2003 **(Maritime Regulations)**	Supporting regulations to the Maritime Act which provides more detail on the regulatory framework.
Operational interference	A new purpose for the Aviation and Maritime Acts, proposed by the Transport Security Bill. This will require critical industry participants to identify, and mitigate against, all hazards that will have a relevant impact on the operation of their business.
Periodic reports	A new requirement proposed under the Transport Security Bill. This will be a way for industry participants to provide periodic update on the continued relevance of their security program.
Relevant impact	The thresholds for hazards to meet the proposed purpose of operational interference. A hazard has a relevant impact if it impacts on the confidentiality, integrity, availability or reliability of the industry participant. Further information thresholds will be

Term	Definition
	finalised in conjunction with industry during the co-design process.
Security assessments	A way for industry participants to consider the threats and risks specific to their operating environment. This will then be used to inform their security program. Security assessments are already a requirement under the Maritime Act.
***Security of Critical Infrastructure Act 2018* (SoCI Act)**	The Act of Parliament that ensures the protection of critical infrastructure (currently focused on port, electricity, gas, and water assets).
Security program	An existing requirement under the Aviation and Maritime Act (also known as transport security program, security program, maritime security plan or ship security plan or offshore security plan). In this document industry participants provide information on how they are meeting the requirements under the Aviation and Maritime Acts.
Security Legislation Amendment (Critical Infrastructure) Bills (SLACI Bill One and SLACI Bill Two)	Two proposed pieces of legislation that will amend the SoCI Act to meet the intent of the critical infrastructure reforms. More information can be found here.
Transport Security Amendment (Critical Infrastructure) Bill 2022	The proposed legislation that will amend the Aviation and Maritime Acts to meet the intent of the critical infrastructure reforms and mirror some amendments proposed in the SLACI Bills.
Unlawful interference	The current purpose of the Aviation and Maritime Acts. Unlawful interference ensures the protection of aviation and maritime infrastructure, goods and passengers from acts, or attempted acts, of terrorism as well as trusted insider threats. The Transport Security Bill proposes expanding unlawful interference to explicitly include cyber security incidents.

Attachment B – Summary of changes and new obligations

Summary of changes for industry participants

Proposed amendment	Aviation industry participants	Maritime industry participants	Critical industry participants
Consideration periods	Yes	Yes	Yes
Operational interference	No	No	Yes
Secretary issued programs	Yes - expanded to include cyber security	Yes – new addition in line with Aviation Act.	Yes – could encompass mitigation against acts of operational interference.
Security assessments	Yes – new addition in line with Maritime Act.	Yes – small change to explicitly require reference in security program.	Yes – will need to encompass acts of operational interference.
Security programs	Yes – include expanded definition of unlawful interference.	Yes – include expanded definition of unlawful interference.	Yes – expanded definition of unlawful interference and operational interference.
Systems testing	No change to current requirements	Yes – new addition in line with Aviation Act.	Yes
Unlawful interference (Cyber Security)	Yes - will need to consider cyber security incidents.	Yes - will need to consider cyber security incidents.	Yes - will need to consider cyber security incidents.

Summary of proposed amendments (with exposure draft Transport Security Bill references)

What's changing	Aviation/Maritime Act reference	Exposure draft Transport Security Bill reference
Critical Industry Participants	N/A	**Aviation Act** Schedule 1 (Part 2) – Item 76 – Insert Division 7 **Maritime Act** Schedule 2 (Part 2) - Item 118 – Insert Division 7AA & 7AB
Improvement notices	N/A	**Aviation Act** Schedule 1 (Part 1) – Item 117A – Insert Division 2A **Maritime Act** Schedule 2 (Part 1) – Item 96 – Insert Division 2A

What's changing	Aviation/Maritime Act reference	Exposure draft Transport Security Bill reference
Information gathering	**Aviation Act** Part 7 **Maritime Act** Part 10	**Aviation Act** Schedule 1 (Part 1) – Item 34 – 80C **Maritime Act** Schedule 2 (Part 1) – Item 64 – 145BC
Powers of aviation and maritime security inspectors	**Aviation Act** Part 5 (Division 2) – Section 79 **Maritime Act** Part 8 (Division 2) – Sections 138 & 139	**Aviation Act** Schedule 1 (Part 1) – Item 34 – 80A **Maritime Act** Schedule 2 (Part 1) – Item 64 – 145BA
Operational Interference	N/A	**Aviation Act** Schedule 1 (Part 2) – Item 75 – Insert Division 5A **Maritime Act** Schedule 2 (Part 2) – Item 117 – Insert Division 5A
Period Reporting	N/A	**Aviation Act** Schedule 1 (Part 1) – Item 47 – Insert Part 6 Schedule 1 (Part 2) – Item 89 – Insert 107AA **Maritime Act** Schedule 2 (Part 1) – Item 90 – Insert Part 9A Schedule 2 (Part 2) – Item 136 – Insert 182AA & 182AB
Persons assisting	N/A	**Aviation Act** Schedule 1 (Part 1) – Item 34 – Insert 80B & 80E **Maritime Act** Schedule 2 (Part 1) – Item 64 – Insert 145BB & 145BE
Relevant Impact	N/A	**Aviation Act** Schedule 1 (Part 1) – Item 10 – Insert Division 4A (9D) **Maritime Act** Schedule 2 (Part 1) – Item 12 – Insert Division 4A (10C)
Relevant Interference	N/A	**Aviation Act** Schedule 1 (Part 2) – Item 74 – Division 4B **Maritime Act** Schedule 2 (Part 2) – Item 116 – Division 4B
Secretary Given Programs	**Aviation Act** Part 2 (Division 6) **Maritime Act** N/A	**Maritime Act** Schedule 2 (Part 2) – Item 123 – after subsection 59B(2) Schedule 2 (Part 2) – Item 126 – after subsection 78B(1A) Schedule 2 (Part 2) – Item 129 – after subsection 100TB(1A)

What's changing	Aviation/Maritime Act reference	Exposure draft Transport Security Bill reference
Security Assessments	**Aviation Act** N/A **Maritime Act** Part 3 (Division 4) – Section 47 Part 4 (Division 4) – Section 66 Part 5A (Division 4) – Section 100G	**Aviation Act** Schedule 1 (Part 1) – Item 18 – after subsection 16(2) **Maritime Act** Schedule 2 (Part 1) – Item 24 – after paragraph 47(1)(a)
Security Directions	**Aviation Act** Part 4 (Division 7) **Maritime Act** Part 2 (Division 4)	**Aviation Act** Schedule 1 (Part 1) – Item 30 – Subsection 67(1) Schedule 1 (Part 2) – Item 87 – After subsection 70(5) **Maritime Act** Schedule 2 (Part 1) – Item 18 – Subsection 33(1) Schedule 2 (Part 2) – Item 119 – After paragraph 33(1)(b)
Systems testing	**Aviation Act** Part 5 (Division 2) – Sections 79 & 80 **Maritime Act** N/A	**Maritime Act** Schedule 2 (Part 1) – Item 52 – at end of subsection 139(2) Schedule 2 (Part 1) – Item 56 – at end of subsection 140A(2) Schedule 2 (Part 1) – Item 61 – at end of subsection 141(2)
Unlawful Interference (Cyber Security)	**Aviation Act** Part 1 (Division 5) – Section 10 **Maritime Act** Part 1 (Division 5) – Section 11	**Aviation Act** Schedule 1 (Part 1) – Item 10 – Insert Division 4A **Maritime Act** Schedule 2 (Part 1) – Item 12 – Insert Division 4A
Use and disclosure of protected information	N/A	**Aviation Act** Schedule 1 (Part 1) – Item 49 – Insert Part 7A **Maritime Act** Schedule 2 (Part 1) – Item 92 – Insert Part 10A

Attachment C – Frequently asked questions

Why are these reforms not in the Security Legislation Amendment (Critical Infrastructure) Bill 2021?

To reflect the established regulatory framework in place for the aviation and maritime transport sectors, both Acts are being amended to ensure that industry participants captured under the reforms can continue to use the existing regulatory framework rather than having two regulatory frameworks that achieve similar results. Industry has provided strong and consistent feedback that leveraging existing regulatory frameworks is preferable to creating parallel regimes

What will the security assessment require and why is this being introduced to the Aviation Act?

The security assessment will give industry participant's freedom to identify and target the threats that are specific to their operating environment. This change will maintain an outcomes-based approach, rather than prescribing threats that apply to all.

The introduction of a security assessment in the aviation sector will align the requirements of a security program with the requirements under the Maritime Act and for responsible entities under the proposed SLACI Bill Two.

What information will the Department want to see concerning 'all hazards' threats?

To ensure that the right balance is found, the regulatory co-design process will explore more detailed thresholds on what type of hazard impacts the confidentiality, integrity, availability and reliability of an industry participant. This detail will be provided in the Regulations and subsequent guidance material that will be issued during the transition period.

Why is the Department expanding its investigation powers and moving to an improvement notice scheme?

Since the Acts were first implemented, the regulatory powers and abilities of Government has progressed significantly. This is recognised in the passage of the *Regulatory Powers (Standard Provisions) Act 2014*, which was passed to ensure greater consistency between different regulatory frameworks and streamlines regulation across the Australian Government. The investigation powers and other new regulatory powers reflect the broader remit of the Acts. While the proposed amendments does include an infringement notice scheme, the Department will continue to support and collaborate with industry as much as possible.

Who will industry participants be required to report cyber security incidents to?

Under the proposed amendments to unlawful interference, all industry participants regulated by the Aviation Act and Maritime Act will be required to report cyber security incidents. These will need to be reported to both the Department and the Australian Signals Directorate (ASD). To limit industry having to report the same information twice, the Department is working with the ASD on ways to support a single reporting mechanism.

What is the threshold for cyber security incidents?

In the Transport Security Bill, the threshold for cyber security incidents is if it has a 'relevant impact' (*Schedule 1 (Part 1) Item 17 – Aviation Act and Schedule 2 (Part 2) Item 16 – Maritime Act*). The threshold and timeframe for reporting a cyber security incident will be informed by industry views through the co-design process and defined in legislative instruments and further guidance material.

Additionally, *Schedule 1 (Part 1) Item 10 – Aviation Act and Schedule 2 (Part 1) Item 12 – Maritime Act* provides further information on the acts or circumstances that need to occur for an incident to be considered a cyber security incident.

When will more detail on what industry participants have to do be provided?

The detail on thresholds and specific requirements that industry will need to meet will be included in the Regulations. The Department will be undertaking a detailed co-design process with industry on the regulatory amendments to ensure that the new requirements are fit for purpose.

My organisation is already regulated against some of these new requirements under other regulatory frameworks. How is this being managed?

The Department will work closely with industry and relevant State and Territory regulators to avoid duplication of obligations. Where an existing framework is in force, the Department is open to leveraging that framework rather than requiring parallel compliance. These matters will be explored in co-design with industry.

What assistance will be provided to support industry participants in uplifting to meet the new regulatory requirements?

The Department acknowledges the potential cost these reforms may have on industry. The Government is not considering financial assistance to industry participants at this stage; instead, the regulatory co-design period will ensure that increased regulatory and administrative burden is kept as low as possible. During the co-design process a full Regulation Impact Statement and Cost-Benefit Analysis will be undertaken.

A security program is approved for up to five years, why does my organisation have to provide a report on the accuracy of the security program during the approved period?

The proposed periodic reporting requirement will allow the Department to ensure the validity of an industry participant's security assessment and security program. Due to the rapidly evolving threat landscape, it is important that the security program is as current as it can be.

Requiring critical industry participants to provide this report annually, reflects the important nature of these industry participants and supports alignment between the Aviation Act and the Maritime Acts with the amendments proposed under SLACI Bill Two.

To keep regulatory burden down for smaller industry participants with a more stable threat environment, non-critical industry participants are only be required to report 30 months after the security program was approved. This aligns with the halfway point of most security programs (which are generally valid for five years or 60 months).

My organisation is about to submit a new security program, is it possible to get more detail on the new requirements now to prevent the need to present another security program in a year's time?

Industry participants need to continue to ensure compliance with the current regulatory framework that is in place until the commencement of the proposed amendments.