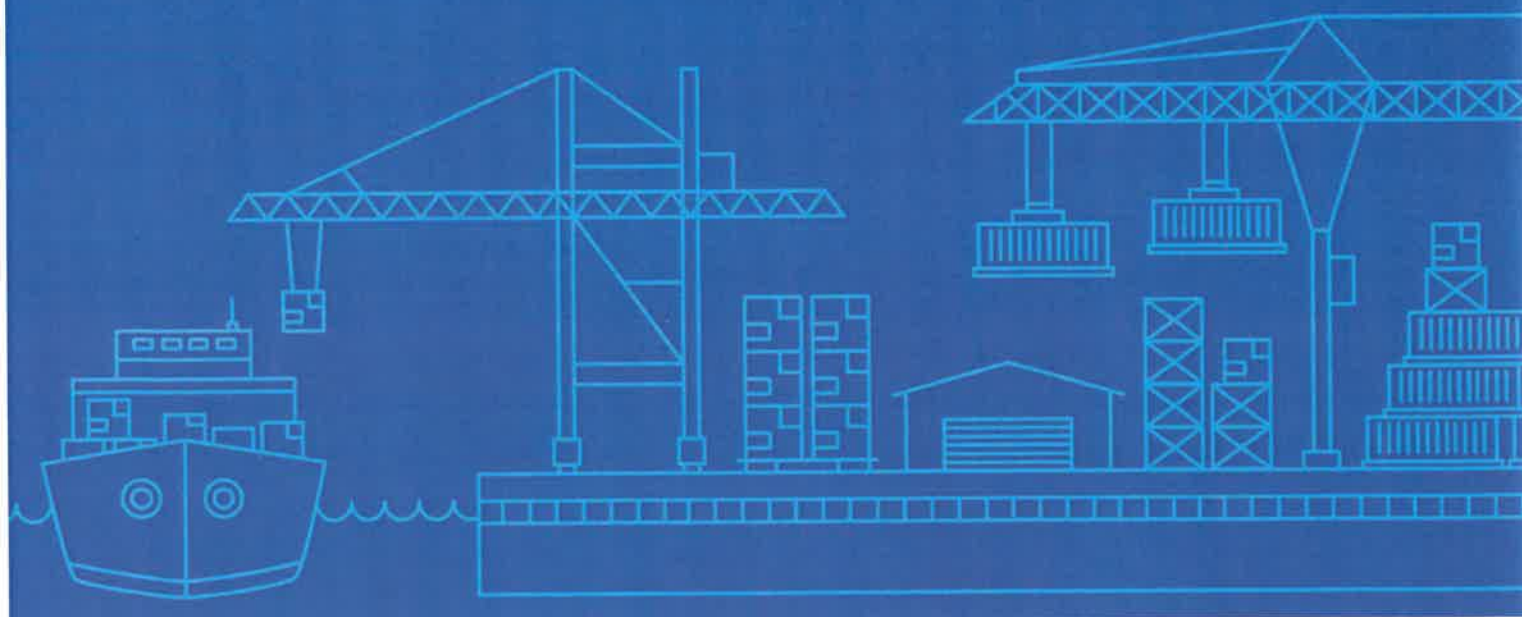




Review of the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024

**Submission to Parliamentary Joint
Committee on Intelligence and Security**

February 2025





Committee Secretariat contact:

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Via: pjicis@aph.gov.au



Ports Australia is the peak body representing the interests of the Australian port industry. It serves as a national voice and plays a crucial role in advocating for policies and initiatives that promote the growth and development of Australian ports.

Ports Australia is governed by a Board of Directors comprising the Chief Executive Officers of 13 port corporations and authorities from across Australia.

We bring together various stakeholders, including government entities, industry members, and representative bodies, to ensure that Australian ports are at the forefront of environmental, safety, and security matters. Ports Australia brings all these groups together in collaboration to ensure our ports are not only in compliance with relevant regulations but go above and beyond to ensure the best outcomes.

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

On 13 January 2025 the Federal Minister for Home Affairs wrote to the Parliamentary Joint Committee on Intelligence and Security referring the *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024* (the Bill) for inquiry and report.

In implementing the reform agenda responding to the Independent Review into Australia's Aviation and Maritime Transport Security Settings, the Bill seeks to amend the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) and the Aviation Act.

Ports Australia welcomes the opportunity to provide to the Parliamentary Joint Committee on Intelligence and Security context to the *Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024* and provide insights into the areas of most interest and concern to our members.

In light of the ownership and operating model differences within the ports and maritime sector, this submission does not represent all industry perspectives.

This response seeks to provide Members of the Committee with an understanding of the broader practical implications and implementation challenges of the measures contained within the Bill that relate to the *Maritime Transport and Offshore Facilities Security Act 2003* (referred to as MTOFSA within this submission). It does not canvas changes to the *Aviation Transport Security Act 2004*, which falls outside the remit of Ports Australia.

The Bill provisions of highest interest or concern to Ports Australia and its members include:

- Expansion of the Act to include cyber security incidents, both attempted and successful, and reporting requirements; including the new definitions of 'cyber security incident' and 'unauthorised access, modification or impairment'
- The intent and impact of Regulations setting 'all-hazards' security obligations, particularly security programs and plans, minimum security standards, security assessments and reporting processes
- Clarity and interpretation of definitions: 'port', 'port facility', and 'security regulated port'
- Clarity and interpretation of definitions: 'unlawful interference', 'relevant impact', 'significant impact', 'relevant interference', and 'operational interference'
- Security directions issued by the Department of Home Affairs.

Engagement by the Department of Home Affairs (the Department) with each port will be important to understand the practical implications and implementation challenges of these measures.

Should the Committee require further details on information provided, please contact Ports Australia.



Ports Australia appreciates the ongoing consultation undertaken by the Department of Home Affairs with the Australian maritime industry on reforms to enhance risk identification, mitigation, management, and action for our port infrastructure across Australia, in an all-hazards approach.

The consultation process leading up to this Bill commenced in May 2024 with the Department releasing the Transport Security Reform Consultation Paper; the *Critical Transport Infrastructure Security Amendment (Security of Australia's Transport Sector) Bill 2024* Impact Analysis Paper; as well as a Supplementary Consultation Paper.

It is noted the Federal Government's stated objectives of the reforms are to ensure:

- government and industry are equipped to respond to current and emerging threats
- industry can meet desired security outcomes, including through identifying, mitigating, and responding to all-hazards threats
- Australia continues to comply with its international obligations relating to aviation and maritime safety.

Ports Australia Overall Recommendations

To maximise the security environment of Australian ports into the future, sustained engagement by the Department of Home Affairs with individual ports across Australia is necessary to understand the nature and experience of each port.

It is essential the Government and the Department of Home Affairs:

- continue to support a fit-for-purpose security legislative framework with evidence-based and cost-effective measures that minimise regulatory burden
- recognise the differing attributes of Australian ports and maritime industry participants, including their existing and proposed security infrastructure; and differing capacity to finance and implement regulatory measures
- assign to industry participants only those responsibilities and financial imposts they should appropriately hold as they undertake that function
- ensure any financial impacts on Australian consumers, exporters and importers are outweighed by the benefits to the Australian community, and
- set a clear regulatory environment for investment certainty.

Maritime industry participants expect, as outlined in this Bill before Parliament, these transport security reforms will require significant resource investment. As maritime and aviation sectors have a critical role in the Australian economy, Ports Australia encourages the Federal Government to consider financial support for industry participants as they implement the changes required.

Regulatory Consistency, Clarity and Certainty, with an Outcomes-based Focus

Ports in Australia are unique in their location, ownership, operating structure, infrastructure, land and landside connections, volumes and types of trade and vessels they service.

In recent years Australian maritime industry participants have been subject to ongoing review and regulatory change, both proposed and realised; resulting in industry uncertainty and resource expenditure on engagement with and responding to the Federal Government and departments; as well as Federal Parliamentary reviews.



Australian governments and businesses must carefully consider their resources and measures available to ensure comparisons between measures are made and adoption is as cost-effective as possible for long term sustainability of Australian trade.

Reform must be based on addressing identified risks and minimising the duplication or redrafting of existing processes, procedures and documentation that remains fit-for-purpose.

It is critical the security framework applied to Australian ports is informed by the current international and national maritime landscape; and provides flexibility to regulation focused on an outcomes-based approach.

As the key interface between maritime and landside trade; port knowledge and experience, legislation, security frameworks, plans and environments need to account for these differences and support each Australian port to optimise their security settings.

Appropriate Identification of Responsible Entity

Port operators, port facility operators and the businesses and structures that support them is essential to shape a suitable and practical plan for securing trade into and out of Australia across the national landscape.

Ports Australia urges all Members of the Australian Parliament and the Federal Government to work with ports and the maritime sector to ensure reforms reflect and respect the appropriate responsible entity in each case given an all-hazards approach to risk management.

In amending legislative and regulatory frameworks, including through this Bill, a critical and overarching imperative is to ensure the identification of the appropriate responsible entity. The imposition of rights, responsibilities and financial costs should be assigned on the entity to which the responsibility should appropriately be held. Accurately prescribing the responsible entity will benefit government and industry in the assignment of positive security obligations and associated accountability.

A considerable but mitigatable risk is held by an entity who is held responsible for obligations that are outside of their control. A responsible entity needs to be the entity best placed to identify, manage, report and act on hazards to physical and operational assets.

As noted earlier, the ownership and operation of port land, infrastructure and facilities differs across the port sector. Some ports are landlord ports which own the land and lease out areas of the land to port facility operators which in turn undertake the day-to-day site management and operations; whilst others own and operate the land and facilities. Others are variations of these.

It is imperative amendments made to legislative and regulatory frameworks, including under this Bill, incorporate the correct delineation between port owners, port operators, facility owners, and facility operators. Each needs their own tailored set of reporting obligations, best reflecting their risk profile – their internal characteristics and the external environment within which they operate.

Where a default setting needs to be included, the default entity is usually most appropriately the port facility operator; with weight given to whether the port operator or port facility operator undertakes day-to-day operations at the port; and whether the port operator has the ability to impact the integrity, availability, confidentiality or reliability of the port facility operator's operations.

One example of entities and responsibilities requiring appropriate and principal distinction is that between a *port facility operator* and a *port operator* (*briefly defined in section 14*).

Currently in the *Security of Critical Infrastructure Act 2018* (SOCI), the port operator is the default responsible entity for a critical port as opposed to the port facility operator; suggesting the port operator is the most appropriate entity to implement positive security obligations under SOCI. It is of substantial concern the port operator is the default responsible entity and suggests the port operator is the most appropriate entity to implement the positive security obligations under the SOCI regime, a regime which in part duplicates that under the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA).



To the extent there is a duplication of obligations between port operators and port facility operators consideration should be given to the appropriateness of the consequences flowing from non-compliance. For example, if a port facility operator is best placed to report a security incident, a port operator might have the same obligations (should it become aware) however it may not be appropriate to make them subject to an offence for not reporting that particular incident.

Landlord ports particularly may not have the degree of insight on risk exposure and accordingly would be unable to adequately address the positive security obligations; as well as ensure the accuracy and quality of reporting to the Australian Government of changes at the port facility owner and operator level.

Ports Australia continues to hold concerns this may undermine the intent of the legislation, to protect Australia's critical infrastructure, if not identified and addressed. It may also carry an unnecessary impost on other entities named as the responsible entity who do not have access to tenant/port facility operator information needed to comply with obligations.

By ensuring the application of any positive security obligations are assigned to the appropriate entity, should they be required; the appropriate entity will be provided with the up-to-date security and risk information, and best practice advice; and any unnecessary regulatory burdens on entities who are not best placed to address these obligations will be eliminated.

All of these outlined factors will assist in the reform objectives being realised in the ports and maritime sector.

Overlapping federal and state regulatory requirements

With most commercial ports in Australia under state or territory government ownership; in establishing a new transport security legislative framework there are practical challenges arising from different legislative frameworks and expectations between jurisdictions (states and territories) and the Commonwealth.

International Context

Internationally owned and operated shipping is crucial to Australian trade. As these vessels are outside of Australia's direct control, security reform within Australia, including MTOFSA, needs to monitor and respond to any significant international decisions affecting security settings and protocols within the maritime industry; including those made in conjunction with the International Maritime Organization, the International Ship and Port Facility Security Code and by international ship owners.





Ports Australia Advice on the Bill before the Parliament

1. Recognising the Crucial Nature of Cyber Security

As part of consultation with industry and stakeholders, the Department in May 2024 released an Impact Analysis Paper highlighting the importance of the aviation and maritime sectors to our community and *“...any avoidance of a disruption that could have otherwise increased the likelihood of significant impacts to aviation and maritime services will have a benefit beyond that of the avoided cost to the economy able to be modelled.”*

Historically MTOFSA has a focus on physical security. Ports Australia and our members support the Bill addressing cyber security challenges within the maritime industry.

It will be crucial for the Department to work with industry participants on the appropriate distinct approaches to both movement in cyber security threats and risk mitigation. For instance, cyber infrastructure may be threatened by newly emerged hacking software released hours ago, where threats to physical infrastructure will often be more static.

Outsourcing information technology (IT) services across all industries is standard; making problematic direct oversight and monitoring of IT systems sufficient in a dynamic all-hazards approach.

Ports Australia would welcome a specific cyber security consultative forum between government and supply chain partners, including the maritime sector, to investigate options to address evolving cyber security concerns and to inform industry of best practice processes. Such a consultative forum could operate similar to, but separate from, the Maritime Industry Security Consultative Forum.

Cybersecurity Reporting Requirements

In amending the MTOFSA framework to reflect the range and scope of emerging cyber security threats to Australian trade, there are challenges with proposals to:

- expand the definition of cyber security incidents
- include actual and attempted cyber incidents
- include ‘unauthorised access, modification or impairment’
- include ‘relevant impact’
- ‘whether direct or indirect’
- have a ‘significant impact’.

Ports Australia and its members note defining through legislation and regulation such terms is projected to require further refinement to ensure there are no unintended consequences.

Wording noted above is subject to interpretation at an executive government, organisational and individual level. Context setting and guidance materials will be important. This is particularly the case in relation to ‘attempted’ cyber incidents in an environment where attempts to access systems with ill-intent are increasingly common. In establishing the new framework it is important the Department does not see industry fail legislative requirements and timeframes through a lack of clarity.

A Single Front Door – Single Point of Reporting and Requirements

The Bill contains varied reporting timelines for separate cyber security incident scenarios.

Ports Australia is concerned over requirements for industry participants to report to both the Secretary of the Department as well as the Australian Signals Directorate’s Australian Cyber Security Centre under the provisions. *Example at proposed Section 171(4).*

Best practice is to establish a ‘single front door’ point of reporting, ensuring an incident report to one area of government is conveyed to all other agencies and departments with a need for visibility of such a report.



Recognising the importance of timely reporting of incidents with a significant impact to the Australian Signal Directorate's (ASD) Australian Cyber Security Centre (ACSC); it is important for the Department of Home Affairs and the ASD to provide appropriate ongoing education and awareness of the differing timelines and the types of incidents, hazards and actions that need to be reported.

2. Expansion of Unlawful Interference (section 11) and Operational Interference (section 11A) to include Attempts

Amending MTOFSA to reflect the range and scope of emerging threats to Australian trade, particularly within cyber security and infrastructure borders, the proposal to expand the definition of unlawful interference as well as operational interference to include attempts will pose challenges in practice.

In establishing the new framework it is important the legislation does not see failures in legislative requirements and timeframes through a lack of clarity. Ports Australia intends to work closely with the Department on providing sufficient guidance and details within the Regulations.

Unlawful Interference that Endangers Life and Infrastructure

Ports Australia recognises the right of individuals to participate in lawful protests and does not seek to limit such rights. It is noted within MTOFSA there is a legislated carve out of:

- "...lawful advocacy, protest, dissent or industrial action that does not result in, or contribute to, an action of..." for unlawful interference (section 11), and
- "...lawful advocacy, protest, dissent or industrial action..." for operational interference (section 11A).

We also note there are existing legislated powers of state and territorial police forces to respond to and act on threats to safety, including from protests and blockades.

In expanding the definitions of unlawful and operational interference it will be important for the Department and enforcement agencies to continue to monitor where the actions of individuals or groups of individuals meet the definition of actual or attempted unlawful interference and/or operational interference and ensure appropriate action is taken.

3. All-hazards security framework

The proposed reforms include a significant expansion in the all-hazards risk assessment, which will apply to all maritime industry participants who are required to hold a Maritime Security Plan (MSP), including port operators; port facility operators; ship operators; offshore facility operators; and offshore service providers.

Both industry and government taking a proactive and holistic approach to risk identification and management; basing actual obligations on the unique operating environment and size of each entity is appropriate.

As stated elsewhere in this document, it is essential to ensure the identification of the appropriate responsible entity so the imposition of rights, responsibilities and financial costs is assigned on the entity to which the responsibility should appropriately be held.

Again, education and awareness of the new requirements will be necessary and key to ensuring widespread compliance with providing to the Department a full analysis of all hazard security risks, potential risk treatments, mitigation measures, and response and recovery strategies.

4. Existing plans and documentation

The Department's stated intent to limit the impost on the industry is acknowledged. To prevent effort duplication and reduce regulatory burden it will be important for the Department to work with industry participants to accept as compliant with reporting requirements, where possible, documents and plans already existing within the entity.



Industry participants should be able to reference updated or expanded versions of internal documents which already consider all-hazards, such as a risk assessment plan or business continuity plan. Entities will also have documents, plans and procedures that comply with jurisdictional emergency management plans, with the scope and extent of which reliant on the hazards identified for their particular site.

5. Broadening the Definition of Security Regulated Port (s13) and clarity on definitional interpretation of 'port', 'port facility' and 'security regulated port'

Division 4—Definitions

port facility means an area of land or water, or land and water, within a security regulated port (including any buildings, installations or equipment in or on the area) used either wholly or partly in connection with one or more of the following:

- (a) the movement, loading, unloading, maintenance or provisioning of security regulated ships;
- (b) the movement of goods that have been, or are intended to be, transported by security regulated ship;
- (c) the storage of goods that have been, or are intended to be, transported by security regulated ship;
- (d) the loading of goods that have been transported by security regulated ship on to another mode of transport;
- (e) the unloading of goods that are intended to be transported by security regulated ship from another mode of transport;
- (f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

Division 6—Security regulated ports and port operators

12 Meaning of port

(1) A **port** is one or more areas of land or water, or land and water, (including any buildings, installations or equipment situated in or on the land or water, or land and water) intended for use either wholly or partly in connection with one or more of the following:

- (a) the movement, loading, unloading, maintenance or provisioning of ships;
- (b) the movement of goods that have been, or are intended to be, transported by ship;
- (c) the storage of goods that have been, or are intended to be, transported by ship;
- (d) the loading of goods that have been transported by ship on to another mode of transport;
- (e) the unloading of goods that are intended to be transported by ship from another mode of transport;
- (f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

(2) A **port** includes:

- (a) areas of water, between the land of the port and the open waters outside the port, intended for use by ships to gain access to loading, unloading or other land-based facilities; and
- (b) areas of open water intended for anchoring or otherwise holding ships before they enter areas of water described in paragraph (a); and
- (c) areas of open water between the areas of water described in paragraphs (a) and (b).

13 Security regulated ports

(1) The Secretary may, by notice published in the Gazette, declare that areas of a port comprise a **security regulated port** if the areas are intended for use either wholly or partly in connection with one or more of the following:

- (a) the movement, loading, unloading, maintenance or provisioning of security regulated ships;
- (b) the movement of goods that have been, or are intended to be, transported by security regulated ship;
- (c) the storage of goods that have been, or are intended to be, transported by security regulated ship;
- (d) the loading of goods that have been transported by security regulated ship on to another mode of transport;
- (e) the unloading of goods that are intended to be transported by security regulated ship from another mode of transport;
- (f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

(2) The notice must include a map of the port that shows the boundaries of the security regulated port.

(3) An area controlled exclusively by the Australian Defence Force must not be included as part of a security regulated port.

The need to secure an area beyond the ship-to-shore interface should be clearly based on identified, measurable risks that can only be addressed through a defined expansion.

In implementing the expanded definitions of 'port', 'port facility' and 'security regulated port' it is critical they are both appropriately prescriptive and carefully considered on a port-by-port basis to avoid unintended consequences. The Department has committed to working with individual ports, and Ports Australia welcomes this commitment.

As outlined elsewhere in this document, each Australian port owns or controls land within the port precinct to a characteristic degree. Establishing a 'security regulated port' on lands beyond the ship-to-shore precinct not within the control and/or ownership of the entity (port corporation / port authority) is highly problematic. For example, the Port Authority for some remote ports have limited or no landholdings beyond the ship-to-shore precinct.

While proposed Section 13 will include standard port infrastructure such as conveyors and cranes; including areas beyond the ship-to-shore interface - such as rail, road and/or pipeline interfaces, intermodal terminals, and remote storage areas/units - may prove problematic. Indeed such areas may be within the ownership or control of another entity, or a jurisdictional (state, territory or local) government authority.

Ports located in major cities and those handling critical export cargo service hundreds or thousands of ships each year will likely have limited interaction by civilians for non-port related purposes. This brings different challenges than regional ports who may handle less than one hundred vessels a year however have large numbers of civilians regularly utilising port infrastructure for recreational purposes, including boating and fishing.



6. Maritime Security Plans (Part 3)

As maritime industry participants will be required to annually review and update Maritime Security Plans (MSPs); which are fundamental to meeting statutory obligations to maintain security at Australian ports; the regulatory framework developed for MSPs (see section 47) needs to be fit-for-purpose, directly address the risks they seek to mitigate, and be outcomes-focused, measurable and enforceable.

Security Assessments and Supply Chain Security (section 47)

47 Content of maritime security plans

- (1) A maritime security plan for a maritime industry participant must:

- (i) set out the participant's measures and procedures for addressing the outcomes of the security assessment included in the plan; and
- (ii) set out the participant's measures and procedures for complying with the minimum requirements (if any) for the participant prescribed by the regulations for the purposes of subsection (4); and
- (ac) set out how the participant will respond to maritime transport or offshore facility security incidents; and

- (3) Regulations made for the purposes of paragraph (2)(b) may prescribe matters for one or more of the following:

- (a) each security assessment;
- (b) each security assessment for a particular kind of maritime industry participant;
- (c) each security assessment for a particular class of a particular kind of maritime industry participant.

- (4) The regulations may prescribe minimum requirements for one or more of the following:

- (a) all maritime industry participants;
- (b) a particular kind of maritime industry participant;
- (c) a particular class of a particular kind of maritime industry participant;

for the purpose of safeguarding against:

- (d) unlawful interference with maritime transport or offshore facilities; or
- (e) operational interference with maritime transport or offshore facilities.

Incorporation by reference

- (5) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of this section and section 48 of this Act may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

Section 47 through Regulation setting, widens the requirement for security assessments, including for ‘...a particular kind of maritime industry participant...’ or a ‘...particular class of a particular kind of maritime industry participant...’.

The use of Regulation to provide context and structure to broadened security assessments will prove challenging to the maritime sector. The Department could limit industry uncertainty by including within the resulting Regulations standardised assessment criteria.

In expanding security assessment requirements, industry participants will need to allocate additional resources to analyse their supply chains to identify and mitigate risks associated with personnel who have remote access to, or influence over, secure areas, security information, or critical systems. The Bill contains no definition of ‘supply chain’, making an industry participant’s defined supply chain contextual to their operations. This has led to uncertainty.

Suppliers of critical, interconnected services such as towage and mooring operators, marine pilot service providers and stevedores are readily informed and engaged in ensuring the security of port facilities and systems.

Noting the range of port operating models and throughputs, assessing the risks posed within both a port’s security controlled activities and their overall supply chain, in particular for critical services and products, and establishing robust mitigation systems will require significant resources by entities.

It is noted in an all-hazards approach there are infrastructure related risks falling outside of the port boundary upon which port operators and/or port facility operators will have no control over their security. Port operations are supported by critical infrastructure including roads including bridges, rail lines, power grids and intermodal terminals.

There are limits to directive controls a maritime industry participant has over a third party supplier in background checking individuals, particularly those based overseas, and to compel their employees applying for or holding a Maritime Security Identification Card (MSIC). Moreover where an individual/s fail



to gain an MSIC, particularly for pre-existing contracts to supply goods or services, the remedies available to cancel or amend the individual/s access to the maritime industry participant's systems remains to be clarified. This may result in contracts having to be amended or cancelled to ensure the maritime industry participant remains compliant; leading to indeterminant financial penalties and expenses.

Developing for industry a plain English guide outlining the requirements for MSICs and/or background checks of individuals within the supply chain would ensure understanding of the requirements individuals will be asked to undertake and answer common questions, including the flow-on implications of someone not meeting security standards.

Ports Australia notes the number of additional individuals who will be required to hold an MSIC or undergo background checks is uncertain. Any delays in the supply of new MSIC cards due to the expansion of the numbers requiring an MSIC is anticipated to require further mitigation measures to be enacted by the Department.

Corporate Governance (including section 59A)

Under the Bill industry participants, with an associated compliance cost, will be required to provide annual attestations from its board or governing body stating all relevant transport security hazard risks have been considered in the risk assessment; proposed control measures address the identified risks, meet legislative requirements, and is within the board or governing body's agreed risk tolerance.

Ports Australia does not oppose the provisions, noting existing corporate governance frameworks and accountabilities of boards and governing bodies. As noted elsewhere, industry participants should not be held responsible for risks, and in turn their mitigation, outside their control and/or knowledge.

Guidance from the Department on acceptable risk parameters to typically consider in risk assessments; and the range of mitigation measures the Department feels are appropriate to reflect; would be of assistance to industry. It will also be important for the Department to ensure ongoing education and awareness programs are developed as effective paths to raise security outcomes over enforcement-centric approaches.

Sections 57A, 59A and 59B and Maritime Security Plan processes

The proposed section 57A permits the Secretary to cancel the Plan, with review rights rested with applying to the Administrative Appeals Tribunal (*section 201*). This contrasts with Section 58 which provides for a show cause process.

Consistent provisions for clear processes to show cause / appeal / defend decisions across Part 3 of MTOFSA would benefit the legislative intent to have industry participants engage positively and with certainty in the development and maintenance of Maritime Security Plans. Ports Australia will continue to work with the Department on clarity during the Regulation making process.

7. Definitions Will be Key

The Bill proposes the expansion and addition of terms within MTOFSA which when implemented must be clear and actionable. Key terms include:

Section 10D	<i>Relevant Impact</i>
Section 10E	<i>Significant Impact</i>
Section 10F	<i>Relevant Interference</i>

10D Meaning of relevant impact

Each of the following is a *relevant impact* of a cyber security incident on a maritime asset:

- (a) the impact (whether direct or indirect) of the incident on the availability of the asset;
- (b) the impact (whether direct or indirect) of the incident on the integrity of the asset;
- (c) the impact (whether direct or indirect) of the incident on the reliability of the asset;
- (d) the impact (whether direct or indirect) of the incident on the confidentiality of:
 - (i) information about the asset; or
 - (ii) if information is stored in the asset—the information; or
 - (iii) if the asset is computer data—the computer data.

10E Meaning of significant impact

An impact (whether direct or indirect) of a cyber security incident on the availability of a maritime asset is a *significant impact* if, and only if:

- (a) both:
 - (i) the asset is used in connection with the provision of essential goods or services; and



- (ii) the incident has materially disrupted the availability of those essential goods or services; or
(b) any of the circumstances specified in the regulations exist in relation to the incident.
- Division 48—Relevant interference**
10F Meaning of relevant interference
- (1) Each of the following is a *relevant interference* with an asset:
- (a) interference (whether direct or indirect) with the availability of the asset;
 - (b) interference (whether direct or indirect) with the integrity of the asset;
 - (c) interference (whether direct or indirect) with the reliability of the asset;
 - (d) interference (whether direct or indirect) with the confidentiality of:
 - (i) information about the asset; or
 - (ii) if information is stored in the asset—the information; or
 - (iii) if the asset is computer data—the computer data.
- (2) Each of the following is a *relevant interference* with the operation of a maritime industry participant:
- (a) interference (whether direct or indirect) with the availability of the operation of the participant;
 - (b) interference (whether direct or indirect) with the integrity of the operation of the participant;
 - (c) interference (whether direct or indirect) with the reliability of the operation of the participant;
 - (d) interference (whether direct or indirect) with the confidentiality of information relating to the operation of the participant.

These three definitions, along with those outlined elsewhere in this Submission and others in the Bill, will require further context and clarity within proposed amendments to the Maritime Transport and Offshore Facilities Security Regulations 2003. Ports Australia and its members anticipate working with the Department to identify these opportunities.



8. Introducing maritime system testing

Introducing an explicit security system testing power under MTOFSA to support maritime security inspectors to perform testing functions is not opposed; however in undertaking such testing it will be important for agencies to ensure the safety and security of persons, vessels and infrastructure is maintained. Ongoing education and awareness in a collaborative environment needs to be the primary goal of all parties.

9. Expansion of Security Direction Powers (section 33)

Ports Australia does not object to the broadening and alignment of the Security Direction powers, as proposed (s33). The Regulations should provide additional clarity on the circumstances and subsequent responses to such directions.

The ports industry consistently works in partnership with the Department of Home Affairs, and in turn the Secretary, to identify and address threats to both the industry and Australia's supply chain, both proactively and in real time.

By responding with proportionality and recognising the existing collaborative relationships it should always be by exception the Secretary would need to issue a Security Direction, to direct an industry participant, in accordance with the CISA Compliance and Enforcement Strategy, to take action to prevent or mitigate the impacts of an act of unlawful interference.

In protecting the community and preventing crime, state and territory police forces have legislated powers to respond to threats to safety, including from protests, blockades, cyberattacks and terrorism. The Department, and in turn the Secretary, when considering whether to issue a Security Direction should remain cognisant of the powers and roles of state and territory police forces and emergency services agencies to respond to incidents of unlawful interference and terrorism. Any potential conflicts between jurisdictional powers and responsibilities must be avoided in establishing a legislative framework where reporting obligations and responses potentially overlap.

Remove requirement for ships operating as both a ship and offshore facility to have two security plans

Ports Australia supports the reduction in regulatory burden by deeming dual purpose vessels to be a security regulated ship, removing the obligation to submit and maintain multiple security plans for the same vessel.



Part 4A - Remove the requirement for a security plan for ships that infrequently travel overseas

Ports Australia supports the proposed amendment of the definition of a security regulated ship to exclude unregulated Australian vessels that intend to travel internationally; noting the intention for such vessels that pass an infrequent overseas voyage test to apply for an exemption from obtaining an International Ship Security Certificate, without the requirement to submit and have approved a security plan.

Maintenance on and refitting of vessels are critical components to maritime safety and where repairs, refitting or maintenance requires a vessel to be relocated overseas; reducing the financial burden and time delays resulting from government processes is supported.

ENDS

