MARITIME INDUSTRY AUSTRALIA LIMITED

Submission to: Dept of Home Affairs

Protecting Critical Infrastructure and Systems of National Significance

Contact: Teresa Lloyd
teresa.lloyd@mial.com.au

About MIAL

Maritime Industry Australia Ltd (MIAL) is the voice and advocate for the Australian maritime industry. MIAL is at the centre of industry transformation; coordinating and unifying the industry and providing a cohesive voice for change.

MIAL represents Australian companies which own or operate a diverse range of maritime assets from international and domestic trading ships; floating production storage and offloading units; cruise ships; offshore oil and gas support vessels; domestic towage and salvage tugs; scientific research vessels; dredges; workboats; construction and utility vessels and ferries. MIAL also represents the industries that support these maritime operators – finance, training, equipment, services, insurance and more. MIAL provides a full suite of maritime knowledge and expertise from local settings to global frameworks. This gives us a unique perspective.

We work with all levels of government, local and international stakeholders ensuring that the Australian maritime industry is heard. We provide leadership, advice and assistance to our members spanning topics that include workforce, environment, safety, operations, fiscal and industry structural policy.

MIAL's vision is for a strong, thriving and sustainable maritime enterprise in the region.

MIAL's overarching position concerning maritime policy in Australia is that we ought to have a sustainable, viable maritime industry. This activity can occur anywhere – coastal, offshore and international. This maritime activity should encompass anything – freight, tourism, passenger movement, port and harbour services, offshore oil and gas, construction, scientific/research, essential services, and government services.

Introduction

It is understood that the Federal Government plans to introduce an enhanced regulatory framework, building on existing requirements under the Security of Critical Infrastructure Act 2018 (the Act). This will include:

- a positive security obligation for critical infrastructure entities, supported by sector-specific requirements;
- enhanced cyber security obligations for those entities most important to the nation; and
- Government assistance to entities in response to significant cyber attacks on Australian systems.

MIALs comments on the questions raised in the consultation paper are provided herein however the overarching comment is that we need to understand much more about who/which entities might be considered critical infrastructure within the maritime context to properly answer many of the questions raised.

Our understanding is that it is not expected to reach too far into foreign ships. This creates two significant issues:

1) Australian ships would then be subject to the additional compliance impost and costs and further erode their ability to complete; and
2) supply chain security cannot be assured unless foreign ships are included since they provide almost the entire sea transport task to, from and around Australia.

Critical Infrastructure – Coverage/Definition (pg 11 – 14)

Extract from consultation paper (highlighting added by MIAL)

The Australian Government's Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

> *'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'* [2]

Within that broad definition of critical infrastructure, the Act currently places regulatory obligations on specific entities in the **electricity, gas, water and maritime ports sectors**. However, entities across all critical infrastructure sectors are facing increasing threats and may require enhanced protections.

These reforms will bring proportionate security obligations to:

- Banking and finance
- Communications
- Data and the Cloud
- Defence industry
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport
- Water.

The intention is for the new requirements will build on and not duplicate existing frameworks. The consultation paper identifies that regulators in those sectors are already equipped to supervise those entities, identify emerging threats, and assist regulated entities respond to those threats.

It is understood that in the maritime space the existing regulation that is intended to be used is MTOFSA.

> *The Australian Government regulates the security of the Australian maritime transport through the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) and the Maritime Transport and Offshore Facilities Security Regulations 2003. This legislation was introduced to meet obligations in response to Chapter XI-2 of the* International Convention for the Safety of Life at Sea 1974 *(SOLAS) and the* International Ship and Port Facility Security Code 2003 *(ISPS).*
>
> *The MTOFSA sets out a regulatory framework which centres on maritime industry participants assessing their operations for security risks, and preparing a security plan which sets out measures to counter these identified risks. Under this framework, security regulated ships, port operators, port facility operators, offshore facilities and offshore service providers are regulated.*

> *The department is responsible for administering the Act and regulations, while maritime industry participants are responsible for delivering security on a day-to-day basis.*

The consultation paper states: "This framework will apply to owners and operators of relevant critical infrastructure regardless of ownership arrangements. This creates an **even playing field** for owners and operators and maintains Australia's existing open investment settings, ensuring that businesses who take security seriously are not at a commercial disadvantage."

In addition, ports are captured by the coverage provisions of the Security of Critical Infrastructure Act 2018. The Act applies to the land that forms any part of the following critical ports.

Broome Port	Port of Gladstone	Port Adelaide
Port of Hay Point	Port of Brisbane	Port of Hobart
Port of Cairns	Port of Melbourne	Port of Christmas Island
Port of Newcastle	Port of Dampier	Port of Port Botany
Port of Darwin	Port of Port Hedland	Port of Eden
Port of Rockhampton	Port of Fremantle	Port of Sydney Harbour
Port of Geelong	Port of Townsville	

The boundary of a critical port is the boundary of a security regulated port under the Maritime Transport and Offshore Facilities Security Act 2003.

Two key issue arises from this:

1) *If supply chain security is a key objective of this initiative, how will MTOFSA deliver that given its very limited application to foreign vessels?*

2) *Some Australian registered passenger vessels are covered by MTOFSA, and there is the ability for some inclusion of foreign passenger vessels. It is not at all clear that vessels of this type should be deemed "critical infrastructure", although it is entirely appropriate that MTOFSA as it stands continues to apply to them.*

Call for views

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

   Without doubt some areas of manufacturing should be considered critical as shown by the COVID-19 pandemic (which saw shortages in sanitiser, face masks, other PPE).

2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

   It seems appropriate.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

One test could be what redundancy exists within the system. For instance, while a service may be undeniably 'critical', if there is more than one operator involved in the activity does that provide some comfort that each individual entity is not in and of itself 'critical'?

6. Which entities would you expect to be owners and operators of systems of national significance?

This needs serious consideration and we would like to be consulted further on the direction the Dept is thinking.

Government-Critical Infrastructure collaboration to support uplift pg 15 - 16

The consultation paper states:

"**Working together**

The Department of Home Affairs will seek to enhance and integrate Government's existing critical infrastructure education, communication and engagement activities, through a reinvigorated TISN and updated Critical Infrastructure Resilience Strategy. This may include a range of activities to improve critical infrastructure and Government's engagement and collective understanding of risk within and across sectors, such as:

- Co-designing **best practice guidance** with entities, government and international partners.
- Improving coordination across Government to provide appropriately classified whole-of-government all hazard **threat assessments and briefings** to entities.
- Using Structured Analytical Techniques such as all hazards scenario planning to improve understanding of risk within and across sectors.
- Drawing on expertise across Government, offering participants **individualised vulnerability assessments**.
- Enhancing Government's existing **research, analysis and evaluation capabilities** to enable ongoing improvements to risk management. This may include dependency modelling, research into evolving risk management practice, and collaboration with academia.
- Ensuring that the **Boards of critical infrastructure entities have visibility** of, and are responsible for planning and actively managing security and resilience.
- Introducing a two-way **industry-government secondment program** to deepen collaboration.
- Improving Ministerial visibility by reporting annually on work undertaken through this partnership.

Call for views

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

For TISN to be effective and beneficial the guidance and advice produced must be practical and targeted.

8. What might this new TISN model look like, and what entities should be included?

For sectors to be engaged effectively the TISN needs to be broken into subsectors so that discussions and work are equally applied to all sectors. For instance, in the transport space, many TISN discussion have previously been dominated by aviation and/or passenger vessels. COVID has shown that the essential nature of shipping and trade requires attention in many areas.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

This is best answered once we know which entities are considered critical infrastructure.

Initiative 1: Positive Security Obligations for Critical Infrastructure (pg 17 – 20)

The consultation paper states:

> The Positive Security Obligation (PSO) will propose a set of principles-based outcomes across Australia's critical infrastructure sectors to protect entities from all-hazards.
>
> As outlined in Figure 1, the PSO will apply to entities designated as '*Regulated Critical Infrastructure Entities*' and owners and operators of '*Systems of National Significance*'.

It goes on to address several issues:

- Principles-based outcomes
- Security obligations
  - **Supply chain security**
    Critical infrastructure entities will protect their operations by understanding supply chain risk. Supply chains can be compromised or disrupted from a variety of natural or man-made activities.
- Regulators

Call for views

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

    There is an inherent fragility within international shipping systems- disruption to the international norms with respect to nations of registration vs nations of operation; inability of the industry to uphold their international obligations for workforce…having greater direct control over those issues by a nation provides security of service.

    Many organisations will not have fully considered supply chain security issues inherent in relying on foreign government regulation of assets and foreign nationals to perform the totality of the sea transport task. Unless the Government plans on ensuring that this is fully investigated, and that there is sufficient expertise to ensure this is done properly, it is perhaps unlikely that the users of shipping services will themselves identify this as a risk, if in fact it is one. In short, unless there is an understanding within Government of the sovereign vulnerability that exists because the vast majority of our sea transport capability is performed by foreign entities, then it is difficult to see how this would be regulated appropriately via the proposed mechanism.

13. What costs would organisations take on to meet these new obligations?

    Entities captured by the various tiers would expect to incur significant additional administrative costs to comply with the proposed obligations.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

Regulators and Enforcement (Pg 21 – 24)

We note that the consultation paper recognises that one size does not fit all approach will not work and that there are various standards and requirements already in place for some sectors.

Call for views

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?
16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

    How does this marry with the idea that TISN would have a role with engaging with entities?
17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

    OTS is the obvious regulators from a security point of view for maritime however the concept of critical infrastructure regulation goes more to ensuring service rather than security *per se*. To that end, there are several regulators in the maritime space that are well versed in shipping regulation. These are the Australian Maritime Safety Authority (AMSA), Dept of Infrastructure, Maritime branch and National Offshore Petroleum Safety Environment Authority (NOPSEMA). We reiterate our earlier point that a much deeper understanding of the fundamentals of international shipping ownership and operation is required than what currently exists to effectively regulate supply chain security.
18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?
19. How can Government better support critical infrastructure entities in managing their security risks?
20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?
21. Do you have any other comments you would like to make regarding the PSO?

Initiative 2: Enhanced security obligations (pg 25 – 27)

We note the issues outlined in the consultation paper that *entity information will be requested by Government on a voluntary basis in the first instance* and that *in the longer term, owners and operators of systems of national significance will be obligated* ***to provide information about networks and systems*** *to contribute to this threat picture if requested*.

We note also the potential for the requirement for independent assessments by third party providers and the co-development of a cyber security play book.

We have no comments on this at this time due to the breadth of operators within our Membership. However, once there is more clarity about which entities will be covered by these requirements it would be possible to provide responses to the questions raised.

Initiative 3: Cyber assistance for entities pg 28 - 30

We note the intention for the Government to invoke two types of powers:

1) Where govt directs entity to take action; and
2) Where the Govt takes action.

As per our comment above, we have no comments on this at this time due to the breadth of operators within our Membership. However, once there is more clarity about which entities will be covered by these requirements it would be possible to provide responses to the questions raised.