Ports Australia

Level 2, 1 York St, Sydney NSW 2000
02 9247 7581 | info@portsaustralia.com.au
www.portsaustralia.com.au

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

Ports Australia appreciates the importance of the protection of critical infrastructure within Australia, to ensure the ongoing social and economic wellbeing, and security of the nation and its people. As Australia is an island nation, ports have and continue to be instrumental in Australia's supply chain, with over 98% of international trade by weight conducted via the country's ports. Accordingly, it is imperative that Australian ports meet appropriate requirements to prevent and mitigate risks and threats, and are appropriately supported to do so, to enable safe, reliable, and efficient trade.

Ports Australia is the peak industry body representing port authorities and corporations, both publicly and privately owned, at the national level. Ports Australia is governed by a Board of Directors comprising the Chief Executive Officers of 14 port corporations from across Australia.

The submission seeks to assist the Department of Home Affairs Critical Infrastructure Centre by providing a ports perspective on the strategic and operational implications of the proposed critical infrastructure reforms. It should be noted that only the questions which Ports Australia has significant feedback on have been addressed.

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)?*

The identified sectors appear to capture the majority of vital functions to Australia's economy, security and sovereignty, however it is imperative that the scope of each sector is defined correctly.

In regard to the maritime ports sector, port owners are currently listed in the *Security of Critical Infrastructure Act 2018*. Port owners are *not necessarily* the owner or operator of the critical infrastructure that sits either entirely or partially within the port e.g. oil pipelines that connect the ship shore interface, to the refinery or storage tank farms. Hence, it is important that consideration be given to defining the appropriate entity which manages or operates the critical infrastructure.

As identified, transport related infrastructure includes ports, airports, roads and rail. During industry consultation for the development of the *Security of Critical Infrastructure Act 2018*, it was raised that waterways, including seabeds and channels are also infrastructure assets and accordingly should be recognised.

Seabeds and channels rely on software for their security and management. Dynamic underwater keel clearance systems provide real-time measurements on the clearance between the bottom of a vessel and the floor of the seabed, taking into account such aspects as the tides, a vessel's size and the cargo weight. Should incorrect data be provided on this clearance, a vessel could attempt to navigate over a seabed it cannot clear, causing potential damage to the seabed, the vessel, the cargo and the surrounding environment.

Vessel traffic information systems (VTIS) are another essential tool used which allow for the protection and safe navigation of channels. A VTIS assists with the safe movement of vessels by providing information on vessels arriving and departing a port and other key information such as hazards. If a VTIS were to provide inaccurate information or fail, such scenarios as a vessel collision in the night could occur. Consequences of this could include vessel, cargo and environmental damage, injury or loss of life, as well as impairment of a ports ability to import and export freight through a shipping channel.

Despite the importance of seabeds and channels being raised during the *Security of Critical Infrastructure Act 2018* consultation, they were not examined further as part of infrastructure. Ports Australia therefore advises that these reforms include seabeds and channels. Whilst seabeds and channels should be recognised, the criticality of each will need to be determined separately.

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

The current definition of critical infrastructure is a broad definition that is still fit for purpose. As detailed in the response to question one above, further scope inclusion may be necessary to highlight the importance of natural enablers such as waterways.

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?*

Ports Australia strongly supports ‘interdependency with other functions’ as a key factor to be aware of and take into account when assessing and prioritising entities and entity classes. Australian ports are varied in their structure being either under public or private ownership, and being either landlord owners, facility owners or facility operators, or a combination of these.

As present, the *Security of Critical Infrastructure Act 2018* requires that the regulated critical infrastructure entities, that is 20 ports in Australia, are required to report on changes to the details of the relevant port facility operators, and are required to do so within 30 days. As port owners do not necessarily own or operate the facilities, they are not always best placed to notify government of these changes. Instead, as port facility operators are directly aware of changes to their own details, they would be better placed to notify government directly should their details change.

In 2017, during consultation for the development of the *Security of Critical Infrastructure Act 2018*, the importance of clearly delineating between port owners, and the owners and operators of the critical infrastructure at a port was raised. As mentioned above, this delineation is significant, as it determines who is best placed to report on obligations. Whilst this was raised by at least one Member of Ports Australia during this consultation period, the *Security of Critical Infrastructure Act 2018* does not appropriately address this delineation.

With the intended reforms, the significance of this delineation will only increase with the introduction of positive security obligations. Landlord ports particularly may not have the level of insight on the exposure of the port facility owners and operators and as such would be unable to adequately address these positive security obligations and keep the Australian Government informed of changes at the port facility owner and operator level. This in itself carries a noteworthy risk and could also constitute an unnecessary impost on such entities.

At present, port operators (owners) and port facility operators are separately defined in the *Maritime Transport and Offshore Facilities Security Act 2003* and it is recommended these definitions be referred to in the reforms to improve the identification of and requirements of regulated critical infrastructure entities.

It is *crucial* that these reforms adequately address the delineation between port owners, facility owners and facility operators. Such revisions would improve the accuracy and quality of reporting to the Australian Government; the application of any positive security obligations should they be required; and reduce any unnecessary regulatory burdens on entities that are not best placed to address these obligations.

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

Currently, port operators and port facility operators are required to have Maritime Security Plans in place, and as part of this potential risks and threats are identified. Risks and threats identified by ports include:

- Natural disaster impacts;
- Pandemics;
- Physical security breaches such as unauthorised access to restricted areas;
- Physical disruptions such as berth channel blockages;
- Physical damages such as intentional or unintentional damage to berth infrastructure;
- Criminal activity;
- Terrorist activity such as bomb threats;
- Drone incursions;
- Biosecurity breaches;
- Environmental hazards such as oil spillages;
- Cyber security breaches and attacks such as ransomware, malware and business email compromise;
- Data breaches, both intentional and unintentional; and
- Information technology system disruptions.

Whilst the reforms aim to capture all threats to critical infrastructure, there is a significant emphasis on the threat of cybersecurity. As ports can face other substantial risks such as environmental threats, more information on how the reforms will address these is also vital and recommended.

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

The Consultation Paper identifies that criticality will be assessed based on interdependency with other functions and the consequence of compromise. Ports Australia supports these proposed criteria.

As outlined in the Consultation Paper it is imperative that further industry consultation is conducted to develop and determine the exact sector-specific criteria and associated assessment methodology. Ports Australia broadly agrees that two aspects which should be taken into account in the sector criteria are an entity's internal characteristics and the characteristics of its external operating environment.

It is *essential* that the sector-specific criteria are sufficiently nuanced to allow for each port to be considered individually, and ensure that considerable regulatory and positive security obligations are not unnecessary placed. For some ports, such obligations could have a significant financial and operational impact.

As advised in the response to question three, ports are often comprised of a number of entities i.e. port landlords owners, port facility owners and port facility operators. Whilst some ports are landlord owners, port facility owners and port facility operators, others are not. Therefore, Ports Australia deems it highly necessary to carefully consider each port structure, and the relationships between the roles within each port structure to ensure that requirements placed on an entity are appropriate and yield the best protection of Australia's critical infrastructure.

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

Entities expected to be owners and operators of systems of national significance may be from a number of sectors, however each entity must be assessed individually. Ports Australia strongly emphasises that only those entities of the utmost criticality should be part of the systems of national significance class.

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

Ports Australia would welcome a revised TISN and Critical Infrastructure Resilience Strategy to support the proposed reforms, with the aims to ensure industry is sufficiently engaged and informed, and that proper collaboration across industry and between industry and government occurs. As part of the Strategy, it is recommended that there be a focus on facilitating collaboration both within industry and with industry and government. This would allow for efficient and effective information sharing, including of best practice and in turn, provide greater resilience across the sector.

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

It is suggested that all regulated critical infrastructure entities as designated with the *Security of Critical Infrastructure Act 2018* are included within TISN, and for those to be divided into subgroups where criticality is similar in nature, and there are direct supply chain synergies.

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?*

Ports Australia would welcome a risk framework for each type of critical infrastructure. Whilst there are common risks across sectors, significant sector specific risks exist and would be best addressed by individual guidance. Guidance on the identification and management of sector interdependencies, information systems dependencies and cyber security best practice would be of benefit.

To avoid any inconsistencies, duplication and potential confusion, Commonwealth and jurisdictional legislation and reporting requirements should be aligned.

Also as referred to in responses to question three and six, currently notifiable event reporting is required by port owners under the *Security of Critical Infrastructure Act 2018*. As port structures vary, sometimes port owners are reporting on the details and notifiable events of third parties i.e. the port facility operator. These obligations need to be reassigned to ensure that reporting is conducted by the party that the notifiable event directly relates to, improving the timeliness and directness of information provided.

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

Ports Australia considers that the principles-based outcomes identified are sufficiently broad to consider all aspects of security risk across the ports sector.

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

The security obligations overall are balanced, however more detail is required and support from the Australian Government pledged to be able to ensure that sectors could meet these requirements. For example, to be able to identify emerging threats as part of 'Endeavouring to safeguard information from common and emerging threats and adhering to best practice guidelines', a 'threat intelligence' capability would be needed. This would be incredibly challenging for industry to meet and come at a substantial cost.

Due to the continually evolving nature of cyber security threats, the provision of ongoing up-to-date guidance on cyber security threat identification, prevention and minimisation measures by the government would be required.

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?*

Ports are already operating in line with these principles. Each port is required to have an approved Maritime Security Plan in place, which requires the active identification of risks, the implementation of measures to prevent and mitigate risks, the practice of security drills and exercises, and strategies to minimise the impact of any realised incidents. Aspects of effective governance are also realised through the Maritime Security Plans, as appropriate security qualifications and incident reporting is required.

Please also refer to the response to question 12.

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

Costs are unable to be quantified at present until a more detailed framework and obligations are provided. It is, however, anticipated that new obligations could require considerable additional resources. In particular, cyber security related costs could be substantial. Please see responses to question 11 and 12 for more information.

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?*

Port are subject to a number of security obligations in-line with these principles, including those outlined in:

- *Biosecurity Act 2015*;
- *Customs Act 1901*;
- *Maritime Transport and Offshore Facilities Security Act 2003*; and
- A number of other federal and jurisdictional legislation and regulation.

Current compliance with these is at a significant cost to the ports. Hence, Ports Australia perceives collaboration between federal and jurisdictional government departments and agencies as vital, to ensure there is no duplication of regulatory oversight or inconsistency of security requirements.

15. *Would the proposed regulatory model avoid duplication with existing oversight requirements?*

The proposed regulatory model *must* be mapped against existing regulation and oversight requirements at the federal and jurisdictional levels to ensure regulatory models are consistent and there is no duplication in oversight and reporting. Compliance with existing requirements needs to be deemed compliant with the proposed regulatory model to avoid duplication.

The *Maritime Transport and Offshore Facilities Security Act 2003* currently provides a regulatory framework for the maritime industry and as part of this, ports are required to meet certain security and reporting obligations. It is recommended that the *Security of Critical Infrastructure Act 2018* and the *Maritime Transport and Offshore Facilities Security Act 2003* are harmonised where possible, however additional obligations *should not* be required of ports that are not regulated critical infrastructure entities.

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?*

The following measures are recommended to be implemented to obtain the best outcomes for the reforms:

- Early and continued sector engagement in the development of sector specific criteria and obligations by the sector regulator, the Aviation and Maritime Security Division of the Department of Home Affairs;
- Accommodation of the need for requirements to complement and not disrupt operational requirements;
- Use of existing industry standards where possible, to avoid duplication and the additional resources required to develop new controls, policies, and processes e.g. Information Security frameworks;
- Clear, unambiguous articulation of requirements;
- Best practice examples of meeting the obligations;
- Industry discussions and cross-sector meetings;
- Up-to-date information around potential threats; and
- Transparency around mitigation systems used to protect identified risks that could impact critical infrastructure of national significance.

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?*

Currently, the Aviation and Maritime Security Division of the Department of Home Affairs is the security regulator for ports and Ports Australia recommends that the Division continue to hold this regulatory role for ports in Australia.

18. *What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?*

Please refer to recommendations made in response to question 16, especially around early and continued sector engagement.

19. *How can Government better support critical infrastructure entities in managing their security risks?*

The provision of guidelines outlining the roles and responsibilities of federal and jurisdictional entities is necessary. These guidelines would need to detail responsibilities around managing and enforcing security risks and requirements, coordination of responsibilities between different parties and up to date key contact details of each party. For example, the coordination between the regulator and relevant jurisdictional authorities including such parties as the police force.

In addition, the provision of up to date intelligence led sectorial risk assessments is necessary. This will allow for a consistent industry approach with entities being able to understand the current risk and security environment for their industry, and to apply their risk management strategies to the current context.

Please also refer to recommendations made in response to question 16.

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?*

Maritime Security Identification Cards are provided through the AusCheck scheme. Individuals are required to have this card to be able to work on vessels (e.g. stevedores, linesman etc.) or within a maritime security zone. The Maritime Security Identification Card is perceived to be sufficient in its risk mitigation of insider threats.

For other port workers, there are differing requirements. Cargo terminal operators, which enter general port areas and do not enter a maritime security zone are controlled under and need to satisfy requirements within the *Customs Act 1901* and associated regulation.

It is suggested that assessment criteria for sectors is aligned where possible.

21. *Do you have any other comments you would like to make regarding the PSO?*

It is imperative that industry is consulted with respect to the design and development of the industry specific Positive Security Obligation (PSO) to ensure it is applicable and practical. Additionally, given the high-level approach to the PSO, clarity is required around the regulators role and ability to define and dictate PSO measures.

The term PSO is used in the *Maritime Transport and Offshore Facilities Security Act 2003*, and effort should be made to have it used consistently.

22. *Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?*

The Department of Home Affairs should undertake preparatory activities to assist in the proactive identification and rapid remediation of cyber vulnerabilities:

- Establishment of an industry government group to educate government on the specific information technology systems that the maritime sector use;
- Establishment of standard information technology related systems and products, which include recognised standards for the identification and remediation of cyber vulnerabilities; and
- Establishment of a national register of approved organisations qualified in responding to cyber incidents for critical infrastructure organisations.

23. *What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?*

With increased information from government, ports within Australia could more efficiently and effectively identify and respond to risks. Information that government holds which would be advantageous to share includes:

- Real-time notification of specific threats and attacks, noting the timeliness and specificity around the threat is imperative *(as set out in the response to question two)*;
- Establishment of standard information technology related systems and products, which include recognised standards for the identification and remediation of cyber vulnerabilities *(suggestion also made in the response to question 22)*; and
- Establishment of a national register of approved organisations qualified in responding to cyber incidents for critical infrastructure organisations *(suggestion also made in the response to question 22)*.

24. *What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?*

Currently ports are required to report on incidents as part of the Maritime Security Plan process. To enable a sector threat picture to be developed and to avoid additional duplicate reporting from industry, details of these incident reports should be drawn on to contribute to the threat picture.

25. *What methods should be involved to identify vulnerabilities at the perimeter of critical networks?*

Ports Australia suggests that government could undertake a range of perimeter network penetration tests of all critical infrastructure entities on an ongoing basis. This would provide consistency of approach, enable timely reporting of possible vulnerabilities to the individual entities, and provide government security agencies with the real-time status of the nation’s security. Moreover, it would reduce costs that the entities might have to bear.

26. *What are the barriers to owners and operators acting on information alerts from Government?*

Ports are inherently interested in the protection of their physical and cyber infrastructure, and would welcome the addressing of barriers to act on government alerts. Barriers currently facing port owner/ operators include:

- Lack of details provided by government about a threat or breach;
- Lack of timeliness by government in notification about a threat or breach; and
- Lack of port owner / operator resources to respond to frequent alerts.

It is important that the above is addressed, and that alerts provided are relevant to each organization alerted, otherwise there is a risk they may be ignored over time.

27. *What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?*

Industry specific playbook templates developed by government in conjunction with industry would be worthwhile. As playbooks need to be specific to an organisation, the playbook template could contain content such as key government contacts, as well as frequently faced scenarios and best-practice examples of responses to a range of scenarios.

28. *What safeguards or assurances would you expect to see for information provided to Government?*

Ports Australia expects that information provided to government will:

- Be treated confidentially;
- Have commercial in confidence status;
- Be kept according to legislative record keeping practices and meet information security requirements; and
- Potentially have immunity, in certain instances.

29. *In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?*

Government should only be able to take direct action in extreme situations of national significance. Meeting such criteria as the below would be necessary:

- Where critical vulnerabilities have been identified in IT systems and services; and
- Where the vulnerability can be exploited; and
- Where is no known control/remedy available; and
- Where the critical infrastructure entity is being attacked for that vulnerability.

Permissible actions might include:

- Short-term block of incoming internet connections from the source of attack (e.g. block internet connections coming from a specific country or region); or
- Short-term slow down/rate limiting of internet speed from the source of the country/region of attack to minimise damages.

30. *Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?*

Ports Australia perceives that the declaration should be driven by the Australian Signals Directorate in conjunction with the Department of Home Affairs.

31. *Who should oversee the Government's use of these powers?*

No comment.

32. *If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?*

As each circumstance may differ, different responses will likely be required.

33. *What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?*

Known legal protections are important to ensure immediate emergency action and transparency. Where acting in accordance with government direction, industry should be afforded immunity and legal professional privilege.

34. *What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?*

No comment.

35. *What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?*

No comment.

36. *Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?*

Ports Australia will be able to comment on this once further obligation details are drafted.