



The Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

DP World Oceania
Level 40, 25 Martin Place
Sydney NSW 2000
GPO Box 4084
Sydney NSW 2000
Tel +61 2 9270 8800
www.dpworld.com/australia
DP World Australia Limited
ABN 27 129 842 093

Dear Sir/Madam,

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

DP World welcomes the opportunity to make a submission in relation to this review. We believe that this review is an opportunity for the Government to update and strengthen the [Maritime Transport and Offshore Facilities Security Act 2003](#) (MTOFSA) and ensure that Australia has robust port protections.

About DP World

DP World is the leading provider of end-to-end supply chain logistics solutions, enabling the flow of trade across the globe. DP World's terminals and industrial logistics parks are strategically located throughout Australia in Brisbane, Sydney, Melbourne and Fremantle, making DP World the leading terminal and supply chain operator in Australia. The terminals and parks offer a comprehensive range of products and services to enhance the efficiency of cargo movement through seamless access to rail, road and sea. As a major 'port operator' under the Bill, DP World is a significant and meaningful stakeholder for the purposes of the Bill.

DP World now contributes to a global portfolio of businesses collectively responsible for more than 10 per cent of global trade.

DP World's services are delivered through an interconnected global network of 128 business units in 60 countries across six continents, with a significant presence both in high-growth and mature markets.

DP World has over 2,000 employees in Australia and more than 108,000 employees worldwide. These employees work with government and other stakeholders along the global supply chain to deliver its world-class port facilities and logistics solutions.

As a leading global logistics provider, DP World plays a critical role in the international supply chain. In November 2023, DP World was impacted by a significant cybersecurity incident, which affected 40% of Australia's import and export capacity.

Our team demonstrated exceptional resilience, successfully restoring operations and clearing over 30,000 containers within just 10 days. This event has reinforced DP World's commitment to enhancing both digital and



DP WORLD

physical security frameworks across our operations. Our insights from this event also give us particular insight and expertise to comment on the Bill.

As threats to global trade continue to evolve, DP World remains focused on implementing robust security measures and innovative solutions to protect our operations, our people, and the vital supply chains we manage, ensuring we maintain our position as a reliable and trusted partner in global trade.

Comments on the Bill

1. Definition of 'port' and 'security regulated port'

The definitions of these terms have been broadened significantly from their existing definitions in MTOFSA. The definition of 'port' for instance, now includes 'any other activity or thing that is critical to ensuring the security and reliability of [a number of listed activities that occur at ports].'

DP World is concerned that this new definition potentially encompasses equipment and facilities outside of a port's site boundaries and the areas that are generally understood to be regulated. For example, an electrical substation or power station might be critical to ensuring the reliability of port operations, but a port operator has no control over these facilities, and they would not be commonly thought to form part of the port. Similarly, it could be argued that a warehouse or depot outside the port boundaries is important for reliable loading of ships etc, which is a port function, but DP World does not imagine that the intention is to capture issues that may arise if say a warehouse or depot is damaged. For example, DP World has inland container depots at sites including Yennora in Sydney, which are entirely separate from the port. As currently drafted, DP World is concerned that the same security obligations that apply to the port would apply to Yennora and such sites, which currently have much lower security arrangements and which are often not managed directly by DP World. This would incur significant capital cost expenses for DP World, and would not achieve any material outcome in terms of port operations as the requirements for such sites are fundamentally different to the requirements for container terminals.

Accordingly, DP World suggests that:

- The definitions are clarified such that the 'port' and the 'security regulated port' must be in the control of/under the control of the port operator; and
- A materiality threshold is included in terms of the impact on port operations.



2. Reporting of cyber-security incidents – new subsection 175(3A)

Under the Bill, a port operator commits an offence if it fails to report a cyber security incident that is likely to have a significant impact on the availability of a maritime asset to the Secretary and the Australian Signals Directorate within 12 hours after becoming aware of the incident.

This obligation duplicates requirements that already exist under other legislation and which requires DP World to report cyber security incidents to the Federal Government. Obligations already exist under the Security of

Critical Infrastructure Act 2018 (SOCi Act). The SOCi Act also contains protections about the information that is provided in an incident report, which provide that this information cannot be used against the provider in any other legal action.

Because of the SOCi Act, the reporting obligation in relation to cyber security incidents is now very onerous and covers several different entities. DP World believes that it is important that the Bill is aligned with the SOCi Act as follows:

- Implementation of reporting on cyber-security incidents to the Federal Government should occur through a single reporting mechanism that covers both SOCi and MTOFSA. This could be portal similar to or part of the existing portal for reporting Maritime Security Incidents. This would also provide simplicity for government as all reports would come to a single reporting centre.
- The same protections that exist in SOCi should be duplicated in the Bill so that they also exist under MTOFSA.
- The Bill should be clear that the penalties under MTOFSA only apply if there have not been penalties under SOCi – it is unreasonable that there is now an additional duplicate offence under Federal legislation.

DP World is also concerned about the breadth of the definition of “significant impact” under the Bill. DP World believes that the Bill should clarify that there are specific circumstances that would not be considered a “significant impact”.

Examples of circumstances which currently could fall under a “significant impact” which DP World considers inappropriate and operationally impractical include:

- Circumstances where services or operations which are impacted can be subcontracted or assigned to another party within the supply chain;
- Circumstances where critical infrastructure or systems are upgraded or onboarded with the intention of improving the supply chain; and
- Circumstances where a disruption is ongoing for less than a period of 10 business days.



DP WORLD

A specific example recently occurring for DP World relates to an industrial relations dispute which caused disruption at the Port Botany Terminal. In this circumstance, DP World successfully collaborated with its competitor, Patricks, in order to mitigate any significant impact to the supply chain. As such, DP World considers that it would not be appropriate for this circumstance – where the issue was appropriately mitigated by assignment to another party - to be captured by the scope of the definition of “significant impact” such that an offence is potentially committed.

3. Interference with assets – definitions and new Division 4A

Under the Bill, there may be requirements for the purposes of safeguarding against operational interference with maritime transport/port facilities where there has been ‘relevant interference’ with an ‘asset’. The Bill contains extremely broad definitions of both ‘relevant interference’ and ‘asset’.

The practical implication of this is that a port operator could be required to take steps to do almost anything that may directly or indirectly affect a huge list of items that may or may not be in the port operator's possession control. There is no control test in the current Bill, and there is also no level of materiality – currently the interference could be any direct or indirect interference with an asset's availability, integrity, reliability; or a confidentiality-breaching interference.

This is operationally unfeasible. The following is required to make these provisions feasible:

- A materiality threshold should be included around the result of the interference;
- The asset should be in the control of the port operator.

4. Division 5A—Operational interference with maritime transport or offshore facilities - Section

11A Meaning of operational interference with maritime transport or offshore facilities

New subsection 11A(1) defines, for the purposes of the MTOFSA, operational interference with maritime transport or offshore facilities to mean, among other things:

- the occurrence of a hazard that results in a relevant interference with the operation of a MIP; or
- the occurrence of a hazard that results in a relevant interference with a maritime asset.

The Bill thereby brings in weather events and similar emergency situations (such as fires) as events that create operational interference and must be mitigated and reported. This raises a number of operational issues, including:

- A lack of clarity around reporting obligations – for example, in the event of multiple lightning strikes, must each strike be reported? Currently, if lightning strikes within a 10-kilometre radius of a port, DP World closes the site down for 30 minutes until the lightning clears, which can happen multiple times in a day. It is not practical to notify each incident, and DP World also imagines that this would put an excessive burden on the Government which would need to review each notification.



DP WORLD

- An extremely low threshold for obligations to be triggered given that 'relevant interference' is so broadly defined – while DP World accepts that sea-borne weather events can cause supply chain outages, it is only fairly extreme events that would have this impact. It certainly would not result from inclement weather in the ordinary course, and even severe weather events can be mitigated operationally.
- A lack of clarity around emergency situations such as localised fires that cause temporary halts to operations but can be mitigated operationally.

In order to make these provisions operationally reasonable, and to avoid duplicated reporting obligations which would put an unreasonable burden on both DP World and Government, at the very least a minimum threshold must be included in the legislation. Guidance should also be provided around what the expectation of Government is in terms of reporting and responding to these events, if those obligations go beyond existing obligations. For example, is DP World required to report on strong winds that might push ships off berths or result in containers being blown over?

In relation to existing obligations, DP World notes that operations at ports already are subject to a regime that results in operations being suspended due to weather events. For example, the harbour master already closes ports where there are adverse weather conditions and can also direct terminals to put out storm lines due to weather that stops operations. Given this regime, DP World questions what is added by including a reporting obligation for such events. As stated above, if a reporting obligation is included thresholds and expectations need to be clarified in the legislation and also at a policy implementation level.

5. Division 6 MTOFSA 59A & 59B - New requirement for annual statements of compliance for maritime security plans

The Bill introduces a new requirement for annual statements of compliance to be given by maritime industry participants to the Secretary for maritime security plans.

This requirement introduces a new operational burden on participants that is of very questionable value to Government. This is because participants are already required to audit their maritime security plans annually in order to comply with MTOFSA. DP World is concerned that this new obligation is a duplication of existing obligations that creates new administrative steps but is simply 'red tape'. DP World thinks deleting this obligation would reduce red tape without in any way impacting security measures.

6. Part 3 of the Bill - Sections 139-141 MTOFSA - Qualifying powers of security inspectors

The amended powers of security inspectors contained in Part 3 of the Bill include system and vulnerability testing, which may cause delays in freight movement. Without clear implementation guidance, these measures could create operational bottlenecks, negatively impacting logistics efficiency.

These new powers could also interrupt operations and/or cause significant damage to operations through the testing. There needs to be an obligation under the Bill for inspectors:



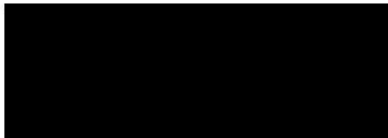
DP WORLD

- To consult with the port operator in the exercise of their powers; and
- To take reasonable measures to ensure that the exercise of their powers does not impact the supply chain or unreasonably interfere with port operations.

Structured industry consultation should be conducted to determine realistic security assessment and system testing obligations that do not disrupt freight operations.

We thank you again for the opportunity to comment on the Bill.

Yours sincerely,



Nicolaj Noes
Executive Vice President
Oceania – APAC
DP World