ALC Submission

Transport Security Amendment (Security of Australia's Transport Sector) Bill
Thursday, 13th February 2025

Introduction

The Australian Logistics Council (ALC) welcomes the opportunity to provide input on the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024. (**the Bill**).

ALC is the peak national body representing major companies participating in the end-to end freight supply chain and logistics industry with a focus on delivering enhanced supply chain safety, efficiency, and sustainability.

As the independent and trusted voice of the sector, ALC supports initiatives that enhance national transport security while ensuring operational efficiency and regulatory certainty for industry participants. This submission outlines the key implications of the proposed amendments on the supply chain sector and provides recommendations to ensure a balanced approach to security and industry sustainability.

The Bill amends the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA), which is designed to enhance the security framework for the aviation and maritime sectors.

ALC makes the following observations:

Expanded Definitions and Security Responsibilities

Industry stakeholders have raised concerns regarding the proposed expansion of the definitions of 'port', 'port facility', and 'security regulated port'. In particular, the broadened definition of 'security regulated port' risks encompassing intermodal centres, remote warehouses, and empty container parks, which are not traditionally subject to the same security considerations as port infrastructure. Extending security regulations to these facilities could introduce unnecessary compliance costs and regulatory complexity without a proportionate security benefit.

It is crucial that maritime industry participants have a clear understanding of their security responsibilities relative to neighbouring Maritime Infrastructure Providers (MIPs). The effectiveness of Maritime Security Plans (MSPs) depends on clear delineation of responsibilities to prevent overlap, ensuring operational efficiency.

Additionally, enforcement mechanisms should be strengthened to support security measures effectively. Robust application of existing legislation is necessary to deter unauthorised access to port security zones, with law enforcement authorities taking a firm stance on penalties for security breaches to maintain the sector's integrity.

All-Hazards Security Assessments

The Bill introduces mandatory cybersecurity incident reporting and all-hazards security assessments, extending the definition of unlawful interference to include cyber threats. While ALC recognises the necessity of strengthening cyber resilience, especially in light of the evolving threat landscape, the proposed measures introduce additional regulatory burdens, increasing compliance costs and operational complexity.

A key concern is the risk of duplication with existing frameworks, such as the *Security of Critical Infrastructure (SOCI) Act* and the *Australian Cyber Security Strategy 2023-2030*, which already impose comprehensive reporting obligations on critical infrastructure operators. To mitigate this, cybersecurity reporting requirements should align with existing legislation to avoid redundancy. Clear reporting thresholds and standardised security assessment templates should be developed to streamline compliance.

The Minister's second reading speech indicated that the all-hazards security framework will require entities to proactively address risks across physical security, personnel security, cybersecurity, supply chain resilience, and natural hazards. This shift reflects a more proactive, holistic approach to managing current and emerging threats, moving beyond a counterterrorism focus.
To reduce the regulatory burden, ALC recommends aligning cybersecurity reporting with existing frameworks to ensure consistency and practicality in compliance.

Cybersecurity Capacity and Workforce Readiness

The Bill's increased obligations will necessitate significant investment in cybersecurity infrastructure, personnel, and training to ensure compliance. However, the existing shortage of skilled cybersecurity professionals presents a significant challenge. Without targeted interventions, industry participants may struggle to meet the Bill's requirements.

ALC recommends government-supported training programs to help businesses meet compliance needs. Flexible, cost-effective options such as online modules will assist in mitigating workforce shortages and alleviating financial pressures. A readily available pool of skilled cybersecurity professionals is essential for the successful implementation of the Bill.

Testing Requirements and Freight Efficiency

The amended powers for security inspectors in Part 3 of the Bill, including system and vulnerability testing, may cause delays in freight movement. Without clear guidance on implementation, these measures could lead to operational bottlenecks, negatively affecting logistics efficiency.

ALC urges that the relevant regulations are circulated with sufficient notice for industry consultation. The Government should carefully consider industry feedback, particularly concerning the workability of proposed regulations and their financial impact.

Further, structured industry consultation is necessary to determine realistic security assessment and system testing obligations that do not disrupt freight operations.

Consultation

Meaningful consultation is essential for shaping transport security reforms. ALC is concerned that the draft amendment Bill was not made available for public consultation prior to its introduction.

While ALC supports efforts to strengthen transport security, regulatory changes must avoid unintentionally burdening the logistics and supply chain sector. A balanced approach is necessary for successful implementation. Ongoing industry consultation is needed to refine security requirements, develop cost-sharing mechanisms that prevent undue financial strain, and provide transitional support to help businesses adapt to new compliance obligations. Addressing workforce readiness and ensuring clear enforcement processes for security inspectors are also critical.

ALC seeks an assurance from the Government that relevant provisions of the Bill will not be proclaimed until adequate consultation has been conducted. Furthermore, exposure drafts of any new regulations, such as revisions to the airport transport security demerit scheme in Part 1 of Schedule 3, should be made available for industry input before finalisation.

Conclusion

ALC recognises the importance of modernising Australia's transport security framework to address contemporary threats. However, regulatory changes must be designed to strengthen security without imposing undue burdens on the logistics sector. Aligning cybersecurity requirements with existing frameworks, ensuring clear guidance on security testing, and addressing workforce readiness are critical to the Bill's effective implementation.

A transparent, consultative approach that incorporates industry feedback will be essential in achieving a secure, efficient, and sustainable transport security regime. ALC looks forward to ongoing engagement with the Government to refine the Bill and ensure its provisions are fit for purpose while safeguarding the efficiency of Australia's supply chain and logistics network.