27 November 2020

Cyber, Digital and Technology Policy Division
Department of Home Affairs
4 National Cct
BARTON ACT 2600

Att: Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure Draft

The Australian Logistics Council (**ALC**) welcomes the opportunity to provide a submission to the Department of Home Affairs on Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure Draft (**the Draft**).

ALC is the peak national body representing major companies participating in the freight logistics industry. Our policy focus is on delivering enhanced supply chain efficiency and safety.

General Comments

ALC recognises the need for the Australian Government to continually review and adapt its approach to protecting the essential services all Australians rely on for our ongoing prosperity, safety and security.

Freight does not stop at state borders, which means that ALC's members bring a national perspective as to how legislation is implemented.

Similarly, ALC's membership is mode agnostic, bringing together perspectives from road, rail, air and sea freight operators, as well as those that provide specific logistics operations such as Australia's exporters and importers.

ALC works with all levels of government to ensure it considers the needs of the logistics industry in its investment and policy decisions. ALC focuses its advocacy efforts on key areas with the aim of improving supply chain efficiency:

- Supply chain logistics safety.
- Infrastructure and regulation.
- Technology.

Its focus on these key issues recognises the importance of efficient supply chains to Australia's economic and social prosperity. High performing supply chains, underpinned by consistent regulation, appropriate national infrastructure and seamless information transfer across the freight logistics industryenables the smooth flow of goods from production to consumption. They are critical to supporting future economic growth, encouraging investment, building more sustainable communities and preparing Australia for future global, national and regional challenges.

The logistics industry is currently subject to regulatory requirements at a federal and jurisdictional level for a range of issues, including cyber security. It is essential that any new federal regulatory requirements regarding the protection of critical infrastructure recognise the existing processes in place in jurisdictions and minimises duplication and the regulatory burden imposed on industry.

As stated on the Home Affairs website:

> the Security of Critical Infrastructure Act 2018 (the Act) seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure'.[1]

As such, the primary purpose of the Act is to safeguard critical assets from aggressive foreign actors – with a primary focus on foreign state actors.

In that context, ALC recommends:

- The expanded definition of Critical infrastructure be limited to the purposes of physical and cyber security and not for broader purposes such as scrutinization of foreign investments.

- Policy makers work with industry to reduce regulatory burden and encourage voluntary declaration of cyberattacks.

- Cyberattacks reported under the legislative tool, are investigated and perpetrators prosecuted where possible.

- Data and information that may be provided by industry be subject to transparency regarding the purpose and use of the information. All sensitive information should of course be subject to strict privacy and confidentiality arrangements, which are made to clear to industry at the outset.

- Government response should be in line with the threat and a blanket approach should not be applied. This should also be considered when applying level of criticality (as defined) to logistics and supply chain assets.

- Logistics operators that are multimodal should be subject to oversight by the one single regulator.

[1] Security of Critical Infrastructure Act 2018 (homeaffairs.gov.au)

ALC finally reaffirms the amendments to the Act proposed in the Draft need to be implemented in partnership with industry to ensure there is no unintentional cumbersome regulatory burden, whilst still achieving the government's cyber security strategy, given the sector is comprised of capital heavy businesses operating with very low profit margins and in an increasingly competitive market.

Conclusion

ALC is committed to working with the Government in the development of any new regulatory framework that seeks to enhance the security resilience of our supply chain in an efficient, effective and affordable manner, and welcomes the opportunity to provide its comments on the Draft.

Should you wish to discuss this submission further, I can be contacted at [redacted].

Yours sincerely,

Kirk Coningham OAM

Chief Executive Officer