AUSTRALIAN LOGISTICS COUNCIL
SUPPLY CHAIN EFFICIENCY AND SAFETY

Critical Infrastructure

July 2022

Critical Infrastructure

Australia is not immune to physical and cyber threats, particularly with increasing geopolitical tensions and the changing global landscape in international affairs. ALC and its members acknowledge the importance and support the intent of the Australian Parliaments recent **Security Legislation Amendment (Critical Infrastructure Protection) Act 2022**. The freight and logistics supply chain are in many respects, advanced in efforts and investment, to mitigate all hazards and cyber risks.

Our focus has been on improving preparedness, ensuring a skilled workforce, and protecting critical assets, to ensure operations can continue and the functionality of the supply chain.

ALC has worked collaboratively with the Department of Home Affairs to bring about pragmatic and sensible amendments to the Act and proposed Risk Management Program rules. Acknowledging significant amendments have been taken on board by the Department and Government including:

- 49 intermodals captured under Critical Freight Infrastructure Assets definition reduced to 13
- Rewording of Critical Freight Services Asset definition to address industry concerns regarding the critical categories of freight and volume (by value)
- Adjustment of start of compliance reporting for Food and Grocery and Critical Freight Services asset classes to commence from January 2023, granting industry a six-month reprieve

Industry is still concerned regarding the drafting of the Risk Management Program rules and the effect this will have on practical application within businesses.

Recommendations

1. The Department of Home Affairs engage in genuine consultation with industry to ensure the rules are fit-for-purpose, pragmatic and can be applied in a way that supports the intent of the Act. The Department to cease calling 'Town Halls' consultation, as it is simply one-way dialogue
2. The Department redraft the rules to remove 'guidelines' and contain these in separate documentation
3. The Department redraft the rules to reflect contemporary risk and cyber security language to ensure there is no confusion in what is required by industry to comply.