AUSTRALIAN LOGISTICS COUNCIL
SUPPLY CHAIN EFFICIENCY AND SAFETY

ALC Submission to Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 and the Associated Risk Management Program Rules Structure

1 February 2022

Introduction

The Australian Logistics Council (**ALC**) welcomes the opportunity to make a submission on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**the Bill**).

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

The interests of ALC's members are interests shared by all Australians - because we all recognise as consumers, customers, businesses and employees the importance of reducing unnecessary costs, strengthening our economy and improving the liveability of our communities.

Our members cover the end-to-end freight and logistics supply chain and include Toll, Linfox, Qube Logistics, DHL Holdings, LINX Cargo Care, Woolworths, Coles and several of Australia's major ports.

This submission will focus on the operation of the risk management plan provisions and in particular the use of the term 'material risk'.

Key recommendations

1. Remove subsection 30AH(8) from the Bill.
2. Re-draft the rules package distributed on 26 November 2021 to clarify what is required and allow businesses to quantify development and compliance costs.
3. The Department of Home Affairs (the **Department**) should reinstate its previous proposal of conducting industry workshops to develop the sector-level rules proposed to be made under paragraph 30AH(1)(c).
4. The Department should, as soon as possible, provide clear information as to the type of information it expects to see provided for inclusion on the Register of Critical Infrastructure Assets.

Please find ALC's detailed rationale in following pages. ALC looks forward to working with the Department to bring about a robust and workable solution, whilst limiting financial and regulatory impost on industry. Please contact [redacted] Director Policy and Advocacy on [redacted] for further information or clarification.

Yours sincerely

[redacted]

Brad Williams
Chief Executive Officer

The Legislative Scheme

The Australian freight and logistics industry supports the Government's goal of ensuring the security of Australia's infrastructure, without placing an undue administrative burden on industry.

We acknowledge the Department has worked with the transport and logistics sector in the development of asset definition rules made under the *Security Legislation Amendment (Critical Infrastructure) Act 2021*, published on 13 December 2021.

We also recognise the changes in the Bill contained in the draft circulated on 21 December 2021 which clarifies:

- that a responsible entity must take all reasonably practicable steps to mitigate relevant risks; and
- when an AusCheck of an individual is required.

The next phase is developing the regulatory structure for risk management programs that are to be developed for the purposes of the critical infrastructure legislation.

These require the amendment to the principal Act proposed in the Bill, by and large the same as those removed from the 2021 legislation when considered by the House of Representatives. ALC reiterates the proposed amendments cannot be considered in isolation from the proposed structure of the Risk Management Program Rules (**rules**).

ALC note there is significant cost and regulatory burden in implementing the principles-based framework. Our members have advised the original cost of developing a risk management plan range from $3m - $10m, depending on the company's level of coverage under the Act, with ongoing compliance costs ranging from $500,000 to $8m per annum. This is not a 'small regulatory impost' as anticipated in the Regulatory Impact Statement for the original 2020 Critical Infrastructure Bill.

ALC assess the reason for this is the legislative design.

A critical risk infrastructure program must relevantly comply with these statutory requirements, set out in proposed subsection 30AH(1):

(1) A ***critical infrastructure risk management program*** is a written program:

(a) that applies to a particular entity that is the responsible entity for one or more critical infrastructure assets; and

(b) the purpose of which is to do the following for each of those assets:

(i) identify **each** hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;

(ii) so far as it is reasonably possible to do so—minimise or eliminate any material risk of such a hazard occurring;

(iii) mitigate the relevant impact of such a hazard on the asset; and

(c) that complies with such requirements (if any) as are specified in the rules.

Paragraphs 576-601 of the explanatory memorandum to the 2020 Bill (the **2020 explanatory memorandum**) sets out what a risk management plan should capture.

They are extensive, as illustrated by this extract from paragraph 583 of the 2020 Bill's explanatory memorandum:

> The impacts of COVID-19 on the availability of workforce and day-to-day operations of an asset are an example of such an unlikely event where there would still be a material risk that would need to be addressed in a critical infrastructure risk management program.

Whilst paragraph 590 of the explanatory memorandum says, in regards to the rules made under proposed subparagraph 30AH(1)(c):

> These rules will be used to provide ***further requirements*** on how the principles-based obligations set out in subparagraphs (1)(b)(i)-(iii) are to be implemented.

For this reason, it is a conceptionally incorrect for any rules made under proposed paragraph 30AH(1)(c) to be merely 'guidance'.

They are a further set of requirements that must be contained in a risk management plan over and above those imposed by paragraphs 30AH(1)(a) and (b)

In particular, proposed new subsection 30AH(7) provides that when considering what is a 'material risk' a responsible entity **must** have regard to the likelihood of the hazard occurring and the **relevant impact** (as defined by the Act) of the hazard on the asset if the hazard was
to occur.

'Material Risk' is not defined in the legislation, although rules may specify:

- a specified risk as a material risk, and
- actions that can be taken to be (deemed as) actions minimising, mitigating or eliminating material risks either generally or with respect to specified critical infrastructure assets.

Proposed subsection 8G(1) defines 'relevant impact' as meaning:

(a) the impact (whether direct or indirect) of the hazard on the availability of the asset;

(b) the impact (whether direct or indirect) of the hazard on the integrity of the asset;

(c) the impact (whether direct or indirect) of the hazard on the reliability of the asset;

(d) the impact (whether direct or indirect) of the hazard on the confidentiality of:

(i) information about the asset; or
(ii) if information is stored in the asset—the information; or
(iii) if the asset is computer data—the computer data.

Proposed sections 30AC-AG require responsible entities to adopt, maintain, comply with, review and update a risk management program and to report annually on the operation of the Plan (**the compliance requirements**), whilst paragraphs 53 – 62 of the of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 Explanatory Document* (the **2022 explanatory document**) sets out the civil penalty consequences of failing to discharge the compliance requirements.

The Regulatory Impact Statement accompanying the 2020 explanatory statement said with respect to the development of risk management plans:

> It is expected that some sectors will already have existing measures in place to manage all hazards and as a result there will only be a small regulatory impost. The costs associated with additional regulation will be further explored in future RIS(s), where detailed economic modelling will be undertaken alongside industry and state and territory governments. [1]

The underlying presumption contained in the first sentence of the extract is that responsible entities would be able to 'cut and paste' from existing risk management documents or from some form of risk management document required under Corporations law[2] into a risk management scheme for the critical infrastructure legislation.

However, as ALC members have said on multiple occasions this is not an accurate presumption.

Sophisticated corporations have risk management frameworks in place.

However, ALC members advise the contingent possibility of prosecution (albeit civil prosecution and not criminal) means their legal advisers will take a conservative view as to what should be in a risk management program.

This means developing a specific plan designed to satisfy the matters that need to be addressed set out in proposed section 30AH and subsection 8G(1) of the principal Act from the ground up.

'Material risk'

[1] Under Part 4.2.1 *Positive Security Obligations*. Pages not numbered.
[2] The only class of corporation required to develop a risk management scheme under the *Corporations Act 2001* are certain financial services corporations. Corporations law does not mandate any ALC member to develop a risk management system – see section 912A of the *Corporations Act 2001*

The term ‘material risk’ is not defined but is well known to the law. There is no reason for the phrase to deviate from its usual usage.

The High Court has indicated a ‘material risk’ is a risk a reasonable person would think, in a particular context, is a significant one[3].

Whilst, as the 2022 explanatory document says it is for the maker of a risk management plan to make that judgement, it remains the case there are a significant number of risks that will need to be identified and managed.

Proposed subsection 30AH(7) reads as follows:

> (7) For the purposes of this section, in determining whether a risk is a material risk, regard must be had to:
>
> (a) the likelihood of the hazard occurring; and
>
> (b) the relevant impact of the hazard on the asset if the hazard were to occur.

It is not definitional in nature.

However, it does mean a plan designer **must,** that is, placed under a mandatory duty, to consider whether a risk is:

1. significant and

2. likely

and then if these tests were satisfied

3. what would happen if the risk was to occur.

Paragraph 598 of the explanatory memorandum to the 2020 Bill purports to explain the **reason** for subsection 30AH(7).

Regrettably it merely explains the reason for subsection 30AH(8), which says that an identified risk is to be treated as being a relevant ‘material risk’.

Paragraph 583 of the memorandum gives somewhat of an example of how the subsection is supposed to work, but there remains no explanation as to the reason for the insertion of the subsection.

[3] *Rosenberg v. Pervical* [2001] HCA 18

Unfortunately, paragraph 67 of the 2022 explanatory document, particularly the phrase:

> The approach to determining what is a 'material risk' is deliberately not prescriptive….and that businesses are best placed to themselves assess what might amount to a material risk…..'

does not assist in explaining the purpose of the subsection.

Rather than clarify what constitutes a material risk in a legal sense, it confuses it.

Subsection 30AH clearly sets out what needs to be done to develop a risk management plan. Adding an additional gloss to what the law understands a material risk to be only adds to confusion as to what is wanted, even if inserted to provide 'guidance'.

ALC recommends that subsection 30AH(7) be removed from the Bill.

A definition of 'material risk' made in rules

The Department published a document called *Risk Management Program Rules* on 26 November 2021. (**the 26 November rules package**)

The package purports to make a 'definition' for what constitutes a 'material risk'.

This 'definition' probably cannot be included in rules made under the Act.

Whilst the legislative intention to extend the capacity to use subordinate legislation to the maximum extent possible[4] it is unlikely a rule can be used to amend what can be have regard to when considering whether a risk is material risk.

This is because:

1. The term material risk is not defined in the legislation.

2. Proposed subsection 30AH(7) of the Act sets out matters take regard of (think about) when determining whether a risk is a material risk.

3. Subsections 30AH(8)-(12) actions that can be taken to be (deemed as) actions minimising, mitigating or eliminating material risks either generally or with respect to specified critical infrastructure assets.

[4] There are 27 signpost references to provisions contained in the *Acts Interpretation Act 1901* and 13 references to a provision contained in the *Legislation Act 2002*

4. Section 61 of the Act allows rules to be made that are necessary or convenient to be prescribed for carrying out or giving effect to the Act. However, as indicated in the Australian Government Solicitor's *Legal Briefing No.102:*

> The (necessary and convenient power) can be used to fill out the framework of the enabling Act and to support its effective operation, but it cannot be used to 'support attempts to widen [its] purposes... to add new and different means of carrying them out or to depart from or vary the plan which the legislature has adopted to attain its ends'.[3] As the High Court has recognised on several occasions: '... in the absence of express statement to the contrary, you may complement, but you may not supplement, a granted power'.[5]

It follows section 30AH contains a code about when rules can be made with respect to material risk.

- For completeness, a capacity for a rule to specify a 'requirement' as contained in proposed paragraph 30AH(1)(c) and specific 'actions' in subsection 30AH(10) can only be read as requiring some form of tangible requirement to be included in an risk management plans and not needing to think (have regards) about something.

In any regard, ALC members have reservations about the material risk 'definition' contained in the 26 November rules package.

The first matter a responsible entity should have 'regard to' when considering if a risk is a material risk is consideration of:

> Impairment of a critical infrastructure asset that may prejudice the social or economic stability of Australia or its people; the defence of Australia or the national security of Australia.

It is acknowledged this mimics the provisions of section 35AB of the Act (inserted by the 2021 legislation) which sets out the grounds when the Minister may give an authorisation to the Secretary of the Department to give directions when a cyber security incident (as defined) occurs.

These criteria are eminently appropriate for this circumstance.

However, ALC members have made it clear that individual businesses, acting within their own sphere of operation, are not the best placed to identify risks identified in the Rule.

[5] https://www.ags.gov.au/publications/legal-briefing/br102

They say that it is not appropriate to burden industry with this responsibility, which it is appropriate given Government has far better information in determining what may constitute something that may (for example) ‘prejudice the social stability of Australia’.

Other elements of the ‘definition’ are also vague.

For instance, one definition proposes that when considering material risk regard should be had to the substantive loss of access to or accidental manipulation of a component of an asset ‘such as’ position, navigation and timing systems’ impacting service provision.

Language like ‘such as’ and then offering a narrow set of examples is unhelpful to a plan designer: is what is after **only** things of a nature of the systems listed or is it **all** components that could impact service provision?

Members advise that the ‘guidance’ in the ‘definition’ only adds complexity and cost to the task of developing a risk management plan that is compliant with the legislative scheme.

Rather than trying to put a ‘definition’ of material risks into a Rule, the Department should use the careful design of the legislation and identify what government precisely wants a risk management plan to cover, designed explicitly against the specific rule making powers contained in subsections 30AH(8)-(12).

General comments on the 26 November rules package

As discussed earlier, the contents of the Bill cannot be considered in isolation from the proposed content of rules as they will impose requirements to include other matters in risk management plans over and above what a business thinks needs to be included to satisfy proposed subsection 30AH(1).

It is acknowledged that the Department is attempting to implement principles-based regulation, to permit responsible entities to identify what is required drawing from their business experience.

However, if this approach is adopted, outcomes must be clearly expressed.

For instance, paragraph 2(a) of Rule 3 contained in the 26 November rules package requires an analysis of how an entity assesses and manages 'unauthorised access, interference or exploitation of the critical infrastructure asset's supply chain'.

Whilst relatively straightforward for assets ('things') falling within the definition of the word in section 4 added by the 2021 legislation, it would be more difficult for critical infrastructure assets that are **networks** that have multiple supply chains.

Another example is Governance Rule 4, which requires responsible entities to how they will take a 'holistic' approach to risk management. Language of this nature makes determining what is required difficult.

A third example is proposed Rule 3.2(c), which asks how 'disruptions and sanctions' due to 'an issue in the supply chain' are managed. It is unclear what this paragraph is asking for.

Finally, there are some examples of duplication.

For example, the requirements of proposed rule 4.1, which requires entities to record how it seeks to minimise and mitigate the impact of physical and natural hazards for 'self-assessed' critical sites is a replication of what is required to be in a risk management plan in the statutory provisions contained in subsection 30AH(1).

It is acknowledged the 26 November rules package are only indicative of policy direction and not drafted with the precision of a statutory instrument prepared by Parliamentary Counsel.

However, proposed paragraphs 30AH(6)(b) and (c) requires the Minister to consider the reasonableness and proportionality of the rules as well as compliance costs when making rules.

As the OECD has indicated:

> There are costs associated with performance-based regulations. They can be difficult to develop, as they require measurement or specification of desired outcomes, which are not always apparent where prescriptive regulation is analysed. Moreover, the very fact that they allow for a range of different compliance strategies suggests that the verification of compliance is likely to be more difficult, and that administrative and monitoring costs may be increased as a result. Similarly, they require the dissemination of sufficient operational guidance to provide adequate understanding and knowledge of the requirements to ensure compliance. Small businesses in particular often do not welcome performance-based regulations, since they can impose a greater responsibility to develop appropriate compliance strategies and create uncertainty as to what is required for compliance.[6]

These comments are also applicable to process-based regulations such as those proposed in the Bill.

The **Attachment** identifies 27 separate things that have to happen under the draft 'rules' in the 26 November rules package – one of the reasons why developing a risk management plan is so costly.

ALC would expect that any risk management plan rules:

1. **Precisely specifies what is wanted.**

2. **Are accompanied by an explanation as to why the specific obligation is being imposed.**

3. **Does not duplicate:**

   (a) **what would be contained in a plan complying with the requirements contained in paragraph 30AH(1)(b) of the Act; or**

   (b) **operational requirements required to be contained on information to be provided for inclusion on the Register of Critical Infrastructure Assets.**

4. **Recognise that Rules for critical freight service infrastructure assets which are networks may require a different design than those applicable to specific places (like an intermodal) that are covered by asset definition rules.**

It is clear the package requires a rethink.

[6] https://www.oecd.org/gov/regulatory-policy/35260489.pdf

The Department previously proposed sectoral based workshops to ‘co-design’ rules that are relevant to the sector whilst providing government with the information necessary to give effect to its mission in ensuring the security of critical infrastructure.

ALC members believe a ‘one size fits all’ approach to developing rules is not efficient and does not satisfy the requirement for the Minister to consider compliance costs as well as the reasonableness and proportionality of the rules set out in proposed subsection 30AH(6).

It is likely there will be a period between the scheduled passage of the Bill in the Autumn Sittings of Parliament and the time a draft set of final rules are exposed for comment as required by proposed section 30AL of the Bill.

The Department should reinstitute its previous proposal of conducting workshops to develop rules proposed to be made under paragraph 30AH(1)(c) of the Act at a sector level

Operational information

Finally, subparagraphs 7(1)(e) and (f) of the Act sets out the 'operational information' to be included on the Register of Critical Infrastructure Assets created by Part 2 of the principal Act, with sections 23, 24 and 25 of the Act imposing an obligation on an asset operator to keep information current.

ALC members report that the definition of what constitutes 'a description of the arrangement under which each operator operates the asset, or a part of an asset' is extremely broad and difficult to interpret.

This is particularly the case for assets that are networks.

The Department circulated to industry notice of the proposal to make rules 'turning on' the requirement to provide information for inclusion on the Register on 16 December 2021.

The Department will need to provide clear guidance as to what it expects to see included on the Register

ALC seeks advice on when the Department proposes circulating such advice for the assistance for those who must undertake the expense of developing of a document containing the operational information to be kept on the Register.

ATTACHMENT

RMP AND OPERATIONAL INFORMATION REPORTING REQUIREMENTS

A. RMP Statutory requirements

1. Identify **each** hazard where there is a material risk that occurrence of the hazard could have a relevant impact on the asset.
2. Identify how relevant hazards can be minimised, eliminated or mitigated.

B. Proposed RMP requirements to be imposed by rules

3. Provide details of a risk-based plan outlining strategies and security controls on how cyber and information security threats are being mitigated.
4. Ensure RMPs complies with standards and frameworks specified in the rules.
5. Set out how critical positions/personnel are identified and who the employees are.
6. Set out how the 'continued suitability' of critical positions/personnel is assessed and managed.
7. Consider requiring AusCheck or equivalent vetting of critical personnel.
8. Set out how risks arising from potential personnel and malicious outsiders causing damage to the functioning of an asset is managed.
9. Set out how risks arising from off boarding personnel is managed.
10. Set out how the supply of products and services to critical assets to enable continued operation is secured.
11. Set out how assesses and manages unauthorised access, interference or exploitation of the assets supply chain, privileged access to the asset by a provider(s) in the supply chain, disruptions and sanctions of the asset due to an issue in the supply chain (sic), vulnerability disclosure for other elements within supply chains, high risk vendors and vendor dependency.
12. Set out how an entity seeks to minimise and mitigate the relevant impact of physical and natural hazards for self-assessed critical sites.
13. Set out how the risk and relevant impacts of unauthorised access, interference and control of critical assets and relevant impact of the natural hazards (sic) are minimised and mitigated.
14. Set out how an entity responds to unauthorised access incidents, controls authorised access, conducts tests to ensure assurance that security measures are effective, how breaches are detected and how the entity will respond and recover from breaches of security.
15. Set out how an entity proposes Minimising and mitigating risks, and how it proposes the asset will recover from impacts arising from relevant impacts arising from natural hazards and disasters, including but not limited to

bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis, health hazards such as pandemics.

16. Ensures an RMP includes a reasonable risk methodology, having regard to ISO 31000 of equivalent standard.
17. Documents the process by which the components of the entity that are essential to the functioning of the asset, the types of relevant impact most significant to the asset and any critical interdependencies with other critical infrastructure assets are identified.
18. Ensure the RMP lists the individuals responsible for the development and implementation of the RMP as a whole, as well as 'the activities detailed within'.
19. Detail how a holistic approach to risk management will be adopted.
20. Outline how an RMP will be reviewed, including what circumstances would require a supplementary review.

C. Operational information requirements

21. List location of asset
22. Description of the area the asset services
23. Name, ABN, address of head office/principal place of business and country of incorporation
24. Name of CEO and country(ies) of which the CEO is a citizen.
25. A description of the arrangements under which each operator operates the asset or part of the asset.
26. Arrangements under which data prescribed by the rules relating to the asset is maintained.
27. Other information as prescribed by the Rules.