AUSTRALIAN LOGISTICS COUNCIL
SUPPLY CHAIN EFFICIENCY AND SAFETY

ALC Submission to The Parliamentary Joint Committee on Intelligence and Security

The Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

25 February 2022

Submission to the Parliamentary Joint Committee on Intelligence and Security on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*

RECOMMENDATIONS

Recommendation 1
That section 30AKA proposed in the Bill be revised or removed.

Recommendation 2
The proposed Rules made under paragraph 30AH(1)(c) be reviewed.

Recommendation 3
The Department should conduct sessions on a sector-by-sector basis to improve the currently proposed prior to the circulation of final draft Rules.

Recommendation 4
The Department cease categorising the conduct of town halls as being 'consultation'.

Recommendation 5
The Government consider an amendment to proposed section 30AH so that a Rule can be made exhaustively establishing the matters to be included in a compliant RMP.

Recommendation 6
The Explanatory Statement accompanying any Rule prepared for the purposes of section 30AH(1)(c) set out the reasons why the Minister believes that imposition of the rule is both reasonable and proportionate.

Recommendation 7
That industry be given at least 12 months from the day a Rule prepared for the purposes of section 30AH(1)(c) is published on the Federal Register of Legislation to prepare an RMP.

Recommendation 8
Funds should be appropriated to the Department of Home Affairs in the 2022-23 Budget to enable a grant or assistance program to aid entities who must develop RMPs.

Recommendation 9
The Department should form a standing group for each of the 11 critical infrastructure sectors identified by section 8D to permit the exchange of information, particularly when amendments to legislation are being proposed.

Recommendation 10
Subject to the proposed amendment to section 30AKA being made, Parliament should pass the Bill.

Introduction

The Australian Logistics Council (**ALC)** welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee)** on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**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, productivity, efficiency and sustainability.

As some ALC members are responsible entities under the *Security of Critical Infrastructure Act 2018* (**the Act**) they have a vested interest in ensuring the regulatory framework is robust whilst being workable and not cost prohibitive to implement.

ALC and its members support the intent of the Bill and of a system that protects Australia's economy (including the operation of its vital infrastructure) from the risk of malicious disruption.

The intention of the ALC membership is to work with government to provide it with the information it needs for it to perform its national security tasks in an efficient, sustainable and effective way.

In this submission, ALC will concentrate on the operation of the risk management plan (**RMP**) process proposed in the new Part 2A to the Act proposed in the Bill.

However, these provisions cannot be considered in isolation from the proposed structure of the Risk Management Program Rules (**Rules**) contained in Attachment C to the Explanatory Memorandum.

As the Minister said in her second reading speech:

> *The government understands that the introduction of reforms that impact many businesses across our economy will cause apprehension. The Government is committed to ensuring that the requirements remain fit for purpose in a dynamic and evolving space.*

Much of the apprehension currently held by ALC members evolve around:

a) an absence of understanding as to how risks are managed by sophisticated businesses; and

b) the poor understanding by government as to how the Proposed new Part 2A of the Act will operate in practice.

Specific feedback regarding the consultation process and industry concerns with the Bill are detailed as follows.

Feedback

The responsiveness to feedback by the Department of Home Affairs (**the Department**) has been mixed.

The Department accepted arguments made by ALC so that only the 12 intermodals critical to the movement of goods are covered by the provisions of the Act, rather than the originally proposed list of 49 intermodals.[1]

It also introduced a rule limiting the scope of the definition of 'critical freight services asset' so only the movement of goods agreed as being critical to the Australian economy were captured.[2]

ALC also acknowledge the Minister recognised in her Second Reading speech that freight services and infrastructure, and food assets will require at least until 1 January 2023 to implement risk management plans (**RMPs**).

It is a costly and complex task for a business operating a network to identify relevant material risks and then develop a risk management process to deal with those risks.

We reiterate that industry will need at least 12 months from the time the RMP Rules are placed on the Legislation Register to develop a compliant RMP.

Finally, ALC is pleased that the Explanatory Memorandum recognises the cost to industry implementing an RMP.

Paragraph 231 of the Explanatory Memorandum recognises that the cost of implementing an RMP imposes an average one-off cost of $9 million per entity followed by an average ongoing cost of $3.7 million per annum to maintain compliance.

The Regulatory Impact Statement that accompanied the Explanatory Memorandum published in 2020 suggested there would only be a 'small regulatory impost'.[3]

The Minister said in her Second Reading speech:

> .... A comprehensive program of consultation has been undertaken with industry to design the rules and definitions that underpin these reforms. From Minister or roundtables that I personally conducted, to official level town halls and working groups, the government has spent over 12 months working in partnership with thousands of entities across industry to ensure that these reforms effectively balanced security with compliance costs.

However, ALC has been somewhat disappointed in the way in which 'consultations' have been conducted since around October.

[1] Schedule 1 to the *Security of Critical Infrastructure (Definitions) Rules 2021*
[2] Ibid, section 9
[3] Under Part 4.2.1 *Positive Security Obligations.* Pages not numbered

'Consultations' have largely been 'Townhall' events held on MS Teams with over 600 people involved, with the only available input the ability to make comments using the Teams chat function and / or responding to prescribed questions via the Menti app.

ALC and its members are of the view these Townhall events do not constitute consultation and were in fact briefing sessions.

ALC also note with the exception of the last Townhall on 4 February 2022, the previous three presentations were identical, demonstrating to industry and the ALC membership, little to no feedback was being taken on by the Department.

In particular, ALC cannot agree that feedback on the structure of the proposed RMP has been taken up.

On 26 November 2021 the Department published what they have subsequently described as being 'policy instructions' or 'drafting instructions' for the RMP Rule draft attached to the Bill's Explanatory Memorandum.

ALC have made several submissions to government voicing concerns about the proposed contents of the Rule as expressed in the document circulated on 26 November, most recently in the submission requested by the Department on version of the Bill circulated on 15 December 2021, with no avail.[4]

ALC has found the best way for its feedback to be received is when the Department works very closely with the sector. This is evidenced by the small roundtables ALC held with the Department between July and November 2021 which resulted in the refining of the Intermodal list and also the redrafting of the critical freight services asset definition.

The Townhall concept simply does not provide industry with the confidence that the 'consultation' conducted is genuine.

Finally, we finally note the Department requested submissions on a draft version of the Bill during December 2021 i.e., the Christmas period, with submissions closing on 2 February 2022.

The Bill was introduced into Parliament on 10 February 2022.

It is therefore difficult to believe that submissions received were considered in any depth.

[4] https://www.austlogistics.com.au/policy-advocacy/alc-submission-2022-alc-submission-to-security-legislation-amendment-bill-2022-and-the-associated-risk-management-program-rules-structure/

The Bill

Proposed sections 30AC-AG of the Act require responsible entities to:

(a) adopt,

(b) maintain,

(c) comply with,

(d) review and

(e) update;

an RMP; and to

(f) report annually on its operation.

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.**

whilst 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.

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[5].

As the Committee can see, significant time and effort must be invested in developing a compliant RMP.

It has been our experience the Department has downplayed the costs involved in developing an RMP, and more generally Departmental officers do not appear to understand how the proposed legislation will work in practice.

This can be implied from the Minister's Second Reading Speech, where she said:

> The risk management program requirement is designed to be incorporated into the existing risk management arrangements. If a critical infrastructure asset looks at and indeed, I hope, exceeds the requirements in the risk management program rules, then this is suitable for fulfilling the obligation. This obligation is meant to be additive to, as well as the least and lightest regulatory impact. Ensuring that there is appropriate risk management in place, such as for cyber and information security, physical and natural hazards, and personnel risks, is increasingly important given the interconnected nature of Australia's critical infrastructure exposes vulnerabilities which, if targeted, could result in significant consequences for our economy, security and sovereignty.

Moreover, as the clause note for proposed section 30AH indicates, an RMP needs to be in writing to ensure:

> Responsible entities are able to determine the most appropriate form for their risk management program, including building on existing enterprise risk management practices.[6]

The underlying presumption inherent in the way that the Department conducted the consultation process is responsible entities would be able to 'cut and paste' from existing risk management documents into an RMP for the critical infrastructure legislation. It has been implied by the Department the contents of the RMP can be drawn from the contents of a 'risk management plan' that needs to be prepared to comply with Corporations Law. However, the only class of corporation required to develop a risk management scheme under the *Corporations Act 2001* are certain financial corporations[7]. Corporations law does not mandate any ALC member to develop a risk management system.

ALC members, being sophisticated businesses, continue to reiterate to ensure their entity can meet the requirements under the RMP a bespoke framework will need to be developed and approved by their respective Boards. This process cannot be shortcut by 'cutting and pasting' from other frameworks. They are purpose design documents.

ALC therefore contends the contents of the second arm of the clause note to proposed section 30AC which reads:

---

[5] *Rosenberg v. Percival* [2001] HCA 18

[6] Explanatory memorandum, paragraph 194

[7] Section 912A

> To reduce the administrative burden for entities responsible for more than one critical infrastructure asset, it is permissible under this section for entities to:
>
> - have a single written program for all Part 2A assets for which they are the responsible entity; or
> - have a number of documents that, in concert, meet the requirements of section 30AH for all Part 2A assets for which they are responsible.[8]

is legally wrong and impractical.

It is legally wrong because subsection 30AH(1) provides that a critical infrastructure risk management program is a written program.

It is impractical because:

(a) ALC members advise that given the number of things that need to be considered in the development of an RMP, it is more efficient to design a new document from scratch rather than determining whether provisions of other risk control documents dealing with specific risks can merely be incorporated into an RMP, noting these are new reporting requirements; and

(b) proposed section 30AH of the Act requires a Board to submit an annual report in relation to the operation of an RMP. ALC members advise the contingent possibility of prosecution (albeit civil prosecution and not criminal) means their legal advisers will take a conservative view and would expect a Board to sign off on the operation of a specific purpose designed document.

We acknowledge the Department is mindful of the burdens the preparation of an RMP can impose, and so the proposed section 30AKA was inserted into the Bill before Parliament. It was not included in the draft Bill exposed in December 2021, therefore this was the first time industry was made aware of this.

It is helpful to compare the proposed section with the relevant clause notes from the Explanatory Memorandum:

[8] Explanatory Memorandum Paragraph 159

Proposed clause	Explanatory memorandum clause note
30AKA Responsible entity must have regard to certain matters in deciding whether to adopt or vary critical infrastructure risk management program etc. *Adoption of program* (1) If an entity is the responsible entity for one or more critical infrastructure assets, then, in deciding whether to adopt a critical infrastructure risk management program, the entity must have regard to such matters (if any) as are set out in the rules. Civil penalty:200 penalty units. (2) Subsection (1) does not limit the matters to which the responsible entity may have regard. *Review of program* (3) If: (a) an entity is the responsible entity for one or more critical infrastructure assets; and (b) the entity has adopted a critical infrastructure risk management program that applies to the entity; then, in reviewing the program in accordance with section 30AE, the entity must have regard to such matters (if any) as are set out in the rules. Civil penalty: 200 penalty units. (4) Subsection (3) does not limit the matters to which the responsible entity may have regard. *Variation of program* (5) If: (a) an entity is the responsible entity for one or more critical infrastructure assets; and (b) the entity has adopted a critical infrastructure risk management program that applies to the entity; then, in deciding whether to vary the program, the entity must have	A key theme of the information received from industry stakeholders during consultation was that the critical infrastructure risk management program obligation needs to be flexible and adaptable to the business processes and environment of an individual responsible entity. To incorporate this feedback into the critical infrastructure risk management program obligation, consistent with recommendation 8 of the PJCIS, section 30AKA is being newly inserted into Part 2A to allow rules to be made by the Minister under section 61 specifying certain matters that must be considered by a responsible entity when adopting, reviewing and varying their critical infrastructure risk management program. *Subsections 30AKA(1)-(2)—Adoption of program* Subsection (1) provides that, if an entity is the responsible entity for one or more Part 2A assets, then the entity must have regard to such matters (if any) that are specified in rules in deciding whether or not to adopt a critical infrastructure risk management program. Breach of the obligation to consider any matters specified in rules under subsection (1) is subject to a civil penalty of up to 200 penalty units. This penalty is a proportionate response based on the nature of the infringement and is designed to align with the obligation to adopt and maintain a critical infrastructure management program under ection 30AC. Subsection (2) indicates that subsection (1) does not limit the matters to which the responsible entity may have regard, clarifying that the entity's obligation to adopt a critical infrastructure risk management program that complies with section 30AH of the SOCI Act is not confined to any matters specified in rules under subsection 30AKA(1). *Subsections 30AKA(3)-(4)—Review of program* Subsection (3) provides that, if an entity is the responsible entity for one or more Part 2A assets and has adopted a critical infrastructure risk management program for those assets, then the entity must have regard to such matters (if any) that are specified in rules in reviewing the critical infrastructure risk management program under section 30AE.

regard to such matters (if any) as are set out in the rules. Civil penalty: 200 penalty units. (6) Subsection (5) does not limit the matters to which the responsible entity may have regard. *Rules* (7) Rules made for the purposes of subsection (1), (3) or (5): (a) may be of general application; or (b) may relate to one or more specified critical infrastructure assets. Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*. (8) Subsection (7) of this section does not, by implication, limit subsection 33(3A) of the *Acts Interpretation Act 1901*.	Breach of the obligation to consider any matters specified in rules under subsection (3) is subject to a civil penalty of up to 200 penalty units. This penalty is a proportionate response based on the nature of the infringement and is designed to align with the obligation to regularly review a critical infrastructure risk management program (that meets the requirements of section 30AH) under section 30AE. Subsection (4) indicates that subsection (3) does not limit the matters to which the responsible entity may have regard, clarifying that the entity's obligation to regularly review a critical infrastructure risk management program that complies with section 30AH of the SOCI Act is not confined to any matters specified in rules under subsection 30AKA(3). *Subsections 30AKA(5)-(6)—Variation of program* Subsection (5) provides that, if an entity is a responsible entity for one or more Part 2A assets and has adopted a critical infrastructure risk management program for those assets, then the entity must have regard to such matters (if any) that are specified in rules in deciding whether or not to vary the program. Breach of the obligation to consider any matters specified in rules under subsection (5) is subject to a civil penalty of up to 200 penalty units. This penalty is a proportionate response based on the nature of the infringement and is designed to align with the obligation to ensure a critical infrastructure risk management program (that meets the requirements of section 30AH) is up to date under section 30AF. Subsection (6) indicates that subsection (5) does not limit the matters to which the responsible entity may have regard, clarifying that the entity's obligation to keep a critical infrastructure risk management program that complies with section 30AH of the SOCI Act up to date under section 30AF is not confined to any matters specified in rules under subsection 30AKA(5). *Subsections 30AKA(7)-(8)—Rules* Subsection (7) provides that rules made for subsections (1), (3) or (5) may be of general application, or relate to one or more specified critical infrastructure assets. A note to this subsection refers the reader to subsection 13(3) of the Legislation Act, which further allows for rules to be made under subsections (1), (3) or (5) in relation to a specified class of critical

	infrastructure assets. Read together, these provisions allow for varying matters to be specified for different types of critical infrastructure assets and industry sectors. Subsection (8) clarifies that subsection (7) does not, by implication, limit the application of subsection 33(3A) of the Acts Interpretation Act. *Draft Part 2A rules* The draft Part 2A rules proposed to be made shortly after commencement of the Bill are at Attachment C and an extract of the Explanatory Statement for those rules is at Attachment D— consistent with recommendation 9 of the PJCIS Report.

The section refers to the 'adoption' of an RMP.

However, proposed section 30AC requires a responsible entity for a critical infrastructure asset to adopt and maintain an RMP. The relevant clause notes to the section in the Explanatory Memorandum read:

> New section 30AC of the SOCI Act provides that an entity that is the responsible entity for one or more critical infrastructure assets to which Part 2A applies (hereon referred to as a Part 2A asset) **must** adopt and maintain a critical infrastructure risk management program that applies to the entity. This requirement will ensure responsible entities develop a nuanced, comprehensive understanding of the hazards and risks that may affect the availability, confidentiality, reliability and integrity of the relevant critical infrastructure asset.
>
> **The purpose of section 30AC is to require responsible entities to develop and keep a written program that satisfies the requirements outlined in new section 30AH.**[9]

There is no discretion as to whether a responsible entity adopts an RMP. It follows the use of the word in the proposed section is curious.

It may well be an attempt to say that the description of the risk contained in a Rule made for the purposes of section 30 AKA need not be contained in a specific RMP document if it is covered in some other risk management document used by the responsible entity. However, it is highly unclear and is regrettably a sign this provision was designed and inserted into the Bill in haste.

[9] Explanatory Memorandum, paragraphs 156-7

The Rules

ALC appreciates the publication of the exposure draft of the proposed rules to be made under proposed paragraph 30AH(1)(c) of the Act in Attachment C to the Explanatory Memorandum. It is disappointing the contents of the 26 November 'policy instructions' published by the Department have been given legal effect.

The clause notes for the paragraph contained in the Explanatory Memorandum reads:

> Under paragraph 30AH(1)(c), the critical infrastructure risk management program must comply with any requirements specified in rules made by the Minister under section 61 of the SOCI Act. Any such rules will be a legislative instrument and publicly available on the Federal Register of Legislation (www.legislation.gov.au). Subsections (2)-(12) provide further clarity as to the scope of this rule making power, including that the rules may be of general application or may relate to one or more specified critical infrastructure assets (subsection (2)).
>
> 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**. Noting the array of critical infrastructure assets that may be subject to the obligation to adopt and maintain a critical infrastructure risk management program, now and into the future, this mechanism will be crucial for ensuring the program is implemented in a risk-based and proportionate manner while still achieving the desired security outcomes and avoiding any unnecessary burden.

It is helpful to compare the structure of section 30AH against a couple of the published rules.

Section 30AH	**Proposed Rules**
30AH Critical infrastructure risk management program (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 practicable to do so—minimise or eliminate any material risk of such a hazard occurring;	**8. Supply chain** (1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act. (2) Beginning on the compliance day, the entity must establish and maintain in the entity's program a process or system that the entity uses to minimise or eliminate the material risk of, or mitigate, the relevant impact of: (c) unauthorised access, interference or exploitation of the asset's supply chain; and (d) misuse of privileged access to the asset by any provider in the supply chain; and (e) disruption and sanctions of the asset due to an issue in the supply chain; and (f) threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and (g) high risk vendors; and

(iii) so far as it is reasonably practicable to do so—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. (2) Requirements specified under paragraph (1)(c): (a) may be of general application; or (b) may relate to one or more specified critical infrastructure assets.	(h) any failure or lowered capacity of other assets and entities in the entity's supply chain. **9 Physical security hazards and natural hazards** (1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act. (2) Beginning on the compliance day, an entity must establish and maintain a process or system in the entity's program: (a) to identify the parts of the asset that are critical to the functioning of the asset (the ***critical sites***); and (b) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a physical security hazard on a critical site; and (c) to respond to incidents where unauthorised access to a critical site occurs; and (d) to control access to critical sites, including restricting access to only those individuals who are critical workers or accompanied visitors; and (e) to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements; and (f) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a natural hazard on the asset. (3) In this subsection: (a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and (b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and (c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program an entity must have regard to: (d) whether the asset's critical sites are described in the program; (e) whether the physical security hazards, the occurrence of which could have a relevant impact on a

	critical site, are described in the program; (f) whether the security arrangements for the asset are described in the program; (g) whether the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the program.

The law makes clear the requirements in the Rules are **in addition** to the quite extensive 'principles based' provisions contained in subsection 30AH(1)(b).

Some of the language is cast in a way that it appears to replicate the RMP requirements set out in the core statutory requirements. For example, the requirements of proposed rule 9 requiring entities to record how it seeks to minimise and mitigate the impact of physical and natural hazards for 'self-assessed' critical sites appears a replication of what is required to be in a risk management plan under paragraph 30AH(1)(b).

Other rules appear either vague or use technical terms out of context. For example, proposed Rule 8 which asks how 'disruptions and sanctions' due to 'an issue in the supply chain' are minimised to ensure there is no relevant impact[10] on a covered asset.

It is generally unclear what this paragraph is asking for in this context and more specifically, members report that disruptions are daily occurrence in the supply chain.

Given that the Rules extend the requirements of what should be in an RMP under paragraph 30AH(1)(b), the level of criticality needs to be defined.

Rule 8(2)(h) also requires the development of a system to manage any failure or lowered capacity of other assets and entities in the entity's supply chain. On face value, it is difficult to determine how a critical freight services asset can determine whether there has been 'lowered capacity' for assets or entities in its supply chain.

Whilst it may be possible to make some observations on how a freight service entity's suppliers and customers maintain their fleet and facility assets it is difficult to see how the entity operating an RMP can determine whether an entity's capacity has been lowered over time.

Finally, ALC members report that it will be difficult to design a compliant RMP for critical infrastructure assets that are networks as they must rely on other parties providing services (such as rail operators moving freight between intermodals) having the systems in place to ensure there are no relevant impacts (as defined) on covered assets.

[10] As that term is defined in section 8G of the Act

MATERIAL RISK

Proposed Rule 4 lists several circumstances taken to constitute a 'material risk' for the purposes of the Act.

For example, Rule 4(a) provides that:

> 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 duplicates the provisions of section 35AB of the Act 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.

Whilst this provision is eminently appropriate for that circumstance ALC members have made it clear that businesses are not best placed to judge when such an impairment has occurred.

It is understood the provision is intended to assist those preparing and RMP in understanding the ambit of what is a 'material risk' for the purposes of the legislation.

However, it is hard to see how the definition assists an RMP drafter in determining what is a 'material risk' for the purposes of satisfying the requirements of subparagraph 30AH(1)(b)(i), something discussed earlier in this submission.

The Department needs to clarify what is the purpose of the inclusion of Rule 4 in the draft rule.

Recommendations

We have observed that it is unclear what section 30AKA is attempting to achieve.

It requires to be amended or removed from the Bill.

Recommendation 1: that section 30AKA proposed in the Bill be revised or removed.

Proposed paragraphs 30AH(6)(b) and (c) of the Act requires the Minister to consider the reasonableness and proportionality of the rules as well as costs of compliance 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.[11]

Paragraph 229 of the Explanatory Memorandum also says glibly that 'security as part of the cost of doing business'.

As indicated at the commencement of this submission, industry fully supports the need for the Government to have the information necessary to ensure risks posed to Australia by the malevolent actions of hostile actors are managed.

However, what is required needs to be clearly indicated. It can't be left to industry to work out what is wanted.

In particular, the proposed Rules are not clear.

The attempt of having a 'one size fits all' set of Rules attempting to cover both independently operating assets and networks has not been successful.

Recommendation 2: the proposed Rules made under paragraph 30AH(1)(c) be reviewed.

The Minister said in her Second Reading Speech that 'additional guidance on how to meet RMP requirements will be jointly developed with 'industry and government partners over the coming weeks and months'.

It is reasonably clear the Rules require refinement. It is not an implementation issue.

The Department previously proposed sectoral based workshops to 'co-design' rules during 2021. That process was abandoned.

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

ALC believes that before a draft set of final rules are exposed for comment as required by proposed section 30AL of the Act, this process should be reinstituted.

As previously discussed, the 'Townhall' model simply does not constitute 'consultation'. It permits the provision of information on a 'top-down' basis but simply does not facilitate the ability for participants to ask the questions that they need to have answered so that they can prepare themselves for the introduction of critical infrastructure legislation in their sectors.

Recommendation 3: the Department should conduct sessions on a sector-by-sector basis to improve the currently proposed Rules prior to the circulation of a revied set of final draft Rules.

Recommendation 4: the Department cease categorising the conduct of town halls as being 'consultation'.

We recognise that the design of the Rules in some way is influenced by a desire to assist RMP drafters in understanding what should be in a program.

However, as discussed as a matter of law they extend the matters that need to be included in an RMP under paragraph 30AH(3)(b).

It is assumed that the Cyber and Infrastructure Security Centre will increasingly have an apprehension of the nature of the risks that need to be managed to meet the challenges of preventing the actions of malicious actors.

ALC members have expressed a clear preference of having to design an RMP satisfying specific requirements established by the Government.

As far as practicable, international standards should be used to specify what is required.

Recommendation 5: The Government consider an amendment to proposed section 30AH so that a Rule can be made exhaustively establishing the matters to be included in a compliant RMP.

It is unusual to have legislation such as paragraphs 30AH(6)(b) and (c) of the Act, which requires the Minister to consider the reasonableness and proportionality of proposed rules to be made under paragraph 30AH(3)(c).

Having regard to the significant number of matters to be considered when designing RMP imposed by paragraph 30AH(3)(b), we believe it is not unreasonable that the Minister publish in the Explanatory Statement accompanying any Rule why the Minister believes a specific rule is both reasonable and proportionate.

Recommendation 6: The Explanatory Statement accompanying any Rule prepared for the purposes of section 30AH(1)(c) set out the reasons why the Minister believes that imposition of the rule is both reasonable and proportionate.

As discussed at the beginning of this submission, industry will need a full 12 months from the finalisation of the Rule so a compliant RMP can be prepared.

Recommendation 7: That industry be given at least 12 months from the day a Rule prepared for the purposes of section 30AH(1)(c) is published on the Federal Register of Legislation to prepare an RMP.

It is important that government has available the information necessary to manage the cyber and infrastructure risks the country faces.

However, that equally means it is essential that government supports industry to develop and implement the risk management plans necessary to meet the international risk environment.

Recommendation 8: Funds should be appropriated to the Department of Home Affairs in the 2022-23 Budget to enable a grant or assistance program to aid entities who must develop RMPs.

Finally, ALC's participation in the Townhall process has illustrated that each specific sector have their own questions that cannot be appropriately answered in a Teams meeting environment.

Section 8D of the Act lists 11 'critical infrastructure' sectors.

Recommendation 9: the Department should form a standing group for each of the 11 critical infrastructure sectors identified by section 8D to permit the exchange of information, particularly when amendments to legislation are being proposed.

However, subject to the proposed amendment to section 30AKA being made, Parliament should pass the Bill.

Recommendation 10: Subject to the proposed amendment to section 30AKA being made, Parliament should pass the Bill.

Thank you for the opportunity to provide a submission to this inquiry, should you have any questions about this submission please contact, Rachel Smith, Head of Government and Policy on [redacted]

Yours sincerely

[redacted]

Brad Williams
Chief Executive Officer

Australian Logistics Council
Suite 17B, 16 National Circuit, Barton ACT 2600
(02) 6273 0755 / admin@austlogistics.com.au
www.austlogitics.com.au | ABN 23 131 860 136

February 2022