ALC Submission

Australian Cyber Security Strategy Cyber Security Legislative Reforms Consultation Paper

Friday, 1 March 2024

The Australian Logistics Council (ALC) welcomes the opportunity to comment on the Australian Cyber Security Strategy Cyber Security Legislative Reforms Consultation Paper (the Consultation Paper), proposing some reforms to the Security of Critical Infrastructure Act 2018 (SOCI).

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.

Freight affects every Australian, every day, everywhere. Common goods purchased by Australians such as food, clothing, household appliances and medicine all need to be transported by freight operators. Australia's population is expected to grow by 10 million by 2040, an increase which must be supported through proactive investment in freight transport and freight logistics infrastructure.

The Australian economy has become increasingly reliant on sophisticated, continent spanning and international supply chain networks. The freight industry serves as the backbone of the economy, facilitating the movement of raw materials, finished products, and essential supplies both within Australia and across the globe.

The supply chain is made up of a highly complex network of interconnected and interdependent parts, with each component playing an essential role in ensuring the smooth and efficient flow of goods and services from a myriad of suppliers to a myriad of end consumers. This comprehensive system involves various entities, including suppliers, manufacturers, warehouses, distributors, retailers, and consumers. Their connections are interwoven through a series of complex set of interdependencies that must work in harmony for supply chains to function effectively.

The productivity and efficiency of a supply chain hinges on the discrete performance and cohesive integration of its various sub-systems. This includes not only freight transport and logistics but also encompasses urban planning and planning regulations, communications, information technology, legal and regulatory systems, and the people and infrastructure that support the process.

Technology is a critical part of this. The Australian Security Intelligence Organisation (ASIO) has issued a stark warning regarding aggressive cyber espionage targeting the nation's critical infrastructure[1]. The annual threat assessment outlined the alarming prevalence of nation-state actors conducting sophisticated cyber reconnaissance on Australian networks and infrastructure. In FY 2022–23, the Australian Signals Directory reported that 21% of the serious incidents (c3 and above) involved companies in the transport sector[2].

This assessment underscores the vulnerability of Australia's critical infrastructure networks to cyber threats and emphasises the urgency of implementing robust cybersecurity measures and strategic reforms to mitigate potential risks of sabotage and disruption.

Comments on the various measures are attached.

Sheena Fardell

Chief of Policy, Australian Logistics Council

[1] https://www.cyberdaily.au/government/10248-asio-director-general-warns-of-nation-state-actors-targeting-critical-infrastructure?utm_source=CyberDaily&utm_campaign=01_03_2024&utm_medium=email&utm_content=1&utm_emailID=b0531c2c0207917a1ccc87a404530f400bdde4199055fa1f7dd0ba630ac9bfc0

[2] https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

Given:

- the nature and number of the proposed consumer goods to be subject to regulation; and
- the possibility that regulated parties may be subject to (amongst other things) monitoring powers contained in the *Regulatory Powers (Standard Provisions) Act 2014*[3]

it is presumed that any compliance duty should be imposed on those responsible for bringing regulated goods into market, rather than users.

It is noted that the United Kingdom legislation referred to in the Consultation Paper (*the Product Security and Telecommunications (Security Requirements for Relevant Connectable Products) Regulations 2023 (UK)* places mandatory security requirements on manufacturers distributors and importers of regulated goods. This would appear to be the sensible place to impose any regulatory liability in this area.

Given Australia imports most of these goods any IoT cybersecurity standard should be those adopted by the majority of comparable nations, such as ETSI EN 303 605 cited in the Consultation Paper.

If the European standard is adopted, consideration should be given to requiring IoT devices to have a mechanism to enable security/firmware patching.

Relevant security settings and configurations should also be enabled by default.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

The addition of a mandatory ransomware reporting obligation is, by definition, an impost on industry imposed at a particularly sensitive and busy time for the business – it has just suffered a ransomware demand.

It is also noted that two reports are proposed to be required – one for when the attack occurs and then a second report if the entity makes a ransomware or extortion payment.

Whilst it may be one thing to require the mandatory reporting of a ransomware event so the Government can have visibility over the national threat picture, it remains the case that it is not illegal for a company to pay a ransom or other form of demand.

It is therefore unclear why a company should, under threat of a civil penalty, be required to make a mandatory report as to why a commercial decision was made to pay a ransom.

Otherwise, the minimum information necessary for the Government to assess the overall threat risk to the Australian economy should be requested when reporting a ransomware demand.

As discussed on page 16 of the Consultation Paper, ALC agrees the time within which a SOCI reporting obligation must be made should as far as possible be the same for all equivalent reporting requirements.

This will assist businesses to socialise within their organisation what a SOCI related event is and when a report should be made and so build appropriate business systems to satisfy the legal obligation.

ALC agrees that if reports are to be made in this area, the law should make clear that making a report does not give rise to any form of legal liability being imposed on the reporter of a ransomware demand and that it will remain lawful for a ransom to be paid, where a company considers it in its interests to do so.

[3] As raised in pages 11-12 of the Consultation Paper

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate

Pages 18 and 19 of the Consultation Paper notes that businesses are becoming reluctant to share information with government and are treating relevant interactions with government as compliance issues dealt with by legal departments.

Unfortunately, that is a function of the level of mandatory reporting and plan development (such as an RMP) requirements the SOCI regime imposes on those subject to the law.

This means that a significantly intrusive legal regime such as SOCI requires to spell out what are the rights, obligations and legal consequences imposed on those subject to the scheme.

It is not entirely clear what 'cyber incident information' is.

The legislation will need to define it, particularly if it meant to be is anything over and above the contents of the proposed mandatory reporting regime[4].

With respect to the proposed 'prescribed cyber security purposes' for the sharing and use of incident information[5], it is difficult to understand why the 'facilitation of consequence management' has been proposed as a relevant purpose.

Neither the ASD nor the Cyber Coordinator has a specific role in 'consequence management' resulting from an individual cybersecurity incident. The concept needs to be better explained, better defined or removed.

As one of the proposed purposes is to provide 'stewardship and advice to industry', the legislation should also make clear that at the very least any information used for this purpose (if not also when information is shared with other government entities) is disseminated on an anonymised basis.

This will be necessary if industry is to be 'incentivised' to provide information to government entities.

For similar reasons, it would not be unreasonable for a 'safe harbour'[6] to be created in relation to information provided to ASD and the Cyber Coordinator, noting that other agencies[7] have powers to take action in relation to matters dealing with the protection and use of personal information.

At the very least the limited use of information proposal canvassed in the Consultation Paper will need to be implemented.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

The Consultation Paper favours a Cyber Incident Review Board that could be used to identify why a breach has occurred, and then share outcomes, that could be based on the Cyber Safety Review Board in operation in the United States[8].

It is noted the US Board is established by Executive Order and not statute[9] and has no powers of compulsion[10].

It may be that a body that is not created by statute may encourage engagement by industry in freely providing information so that broader 'lessons can be learned'.

If a mechanism is to be created in the law, a more straightforward legislative design would be something like that contained in the *Inspector of Transport Security Act 2006*, which contains all the powers that would facilitate the publication of the reports necessary to advise how industry can reduce cyber risk.

[4] Including voluntarily supplied information

[5] CP:20

[6] As discussed on CP:19

[7] Such as the Office of the Australian Information Commissioner

[8] CP 22

[9] https://www.cisa.gov/sites/default/files/2023-09/CSRB%20Charter%2009.21.2023%20APPROVED_508c.pdf

[10] https://www.cisa.gov/sites/default/files/2024-02/CSRB%20FAQs_02022024_508c.pdf

If the Air Transport Safety Board model is to be adopted, it is recommended that the threshold of a review be limited to circumstances where either national security or the efficient operation of the Australian economy is involved.

ATSB investigations are costly and complex and can be for businesses involved very time consuming and intrusive.

A high threshold is therefore necessary to ensure that a 'lessons learned' mechanism is directed towards providing advice where any weaknesses in cyber management can lead to impact on the country as a whole.

This will particularly be the case if it is proposed to require questions to be answered by a person.

At the very least a provision similar to section 27 of the *Transport Safety Investigation Act 2003*, which provides a report is not admissible in evidence in any civil or criminal proceedings, will need to be included if parties are to be encouraged to engage in an inquiry.

The legislation should also require that any 'lessons learned' report should only contain deidentified information. Governments must always remember the reputational risks that companies face simply by being assessed and named into the public place.

Finally, it should be noted that the powers proposed to be given a 'CIRB' discussed on page 27 of the Consultation Paper are not 'modest'.

They are quite intrusive, and their existence may lead parties who may fall subject to the review to deal with any inquiry as a compliance/legal issue and so make the inquiry process not as fruitful as hoped.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

The concept of 'business critical data' is very vague.

In one sense, all data that is available to an entity to make business decisions or provide data is 'critical' to the business.

Whilst page 37 of the Consultation Paper indicates the risk management plans that must be developed under SOCI are 'principles-based', as ALC has said in other submissions made relating to SOCI:

> *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].

A greater explanation as what is contemplated as being 'critical business data' is required.

As the Consultation Paper also indicates, all businesses have obligations under the Privacy Act 1988 to protect information.

It is recommended that a close analysis is undertaken to ensure that obligations imposed by the Privacy Act, or any other piece of legislation is not duplicated in SOCI.

It is costly for business to comply with the provisions of different pieces of legislation that are nearly the same, but marginally different. Only one piece of legislation should set out the rights and obligations of businesses in one policy area.

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

ALC finally expects that any explanatory memorandum accompanying legislation introduced into Parliament will attempt to quantify the business and compliance costs imposed by the introduction of this additional component of a SOCI risk management plan as anticipated by the *2023 Australian Government Guide to Policy Impact Analysis*.

Measure 6: Improving our national responses to the consequences of significant incidents – Consequence management powers

It is noted the intention of introducing powers to require parties to do certain things as directed because of a cybersecurity incident is perceived as being a further enhancement on the scheme established by Part 3A of SOCI.

The issues relating to the costs involved in having to comply with a multiplicity of statutory provisions dealing with the same policy area discussed above are also relevant here.

Given the intrusive nature of the types of directions that are anticipated as being able to made (such as those discussed in the hypothetical scenario relating to the supply of chlorine gas discussed on page 45 of the Consultation Paper) the legislation must make powers should only be exercised where:

- the relevant cybersecurity risk poses a significant risk to either national security or the Australian economy; and
- all other legislative provisions dealing with emergency management have been exercised or are insufficient to deal with the particular risk.

The legislation should also require the reasons for the exercise of this power and how the power was exercised to be tabled in Parliament as soon as practicable.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

ALC has no particular comment in relation to this measure (particularly as it relates to when protected information can be shared within government), other than to observe that moving towards a 'harms-based' approach may also complicate decision-making processes, as entities must assess potential harms to various interests, including security, commercial interests, and public welfare.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

ALC notes that when the amendments to SOCI were being discussed in 2022, the point made by government was that industry was in the best position to determine the contents of a risk management plan. That was the rationale for the legislation requiring a plan to be made to be framed in a 'principles based' manner.

It is assumed the Government now considers it has the internal capacity to determine when a written plan developed for a particular business is 'seriously deficient'[12].

The procedural fairness provisions requiring an entity be given an opportunity to respond to an intention to impose a direction is acknowledged, however a provision allowing for an external merit review of a decision to impose a direction to vary a plan will need to be included.

This is an appropriate inclusion given the decision under review would be the competency of a plan and does not relate to a real-time cybersecurity risk that requires immediate management.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

ALC has no comment on this measure.

[12] The language used at CP:52. The other thresholds before the direction making power may be exercised are satisfactory.