Submission by the Australian Information Industry Association

To the Parliamentary Joint Committee on Intelligence and Security

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and the operation, effectiveness and implications of the *Security of Critical Infrastructure Act 2018*

12 February 2021

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:

• providing a strong voice of influence

• building a sense of community through events and education

• enabling a network for collaboration and inspiration; and

• developing compelling content and relevant and interesting information.

We represent a larger number of technology organisations in Australia, including:

• Global corporations

• Multinational companies

• National organisations; and

• a large number of small and medium businesses, start-ups, universities and digital incubators.

Introduction

The AIIA has indicated its support for the expansion of sectors that are defined in this bill as critical infrastructure sectors and fall under this regulatory scheme. The Department of Home Affairs' 2020 review of critical infrastructure (**CI**) and the preceding consultation paper recognised the digitisation of our economy and resultant increase in cyber threats. We acknowledge that the government is seeking to extend a regulatory framework across 11 critical sectors and their attendant systems in order to protect key supply chains and infrastructure of national importance in the event of a serious security threat, and understand the rationale. The AIIA acknowledges the significance of CI legislation as a policy response for the defined critical sectors, with oversight in terms of their cybersecurity sending a strong market signal and driving investments accordingly for those cloud and other sectors in line with this policy direction. However, the AIIA calls on government and the Joint Committee on Intelligence and Security to ensure that the Critical Infrastructure regime operates on the basis of rules that are genuinely co-designed, flexible, and give rise to regulation that is not burdensome or duplicative in nature.

Any action taken by the Government through the Department of Home Affairs or the Australian Signals Directorate in relation to critical infrastructure entities in the event of a cybersecurity incident could have reputational impacts as well as impacts upon customers, which needs to be considered by the relevant Secretary and Minister in analysing downstream effects of declarations and interventions. Many of the customers of critical infrastructure entities will have obligations themselves that they may want to pass onto the

entity in turn, which needs to be considered, as well as ensuring that customer contracts address potential implications of the reforms, for example the potential need for the entity to provide access to infrastructure to the Australian Signals Directorate, which could have contractual implications with customers. These contractual and customer-facing impacts should be considered by the Committee, and appropriate amendments made to remedy these concerns.

Regarding the direct action power in regards to the data and processing sector, the AIIA is calling for appropriate appeal mechanisms, the opportunity for judicial review, and the ability to refer disagreements to an independent expert panel to ensure appropriate recourse. This is discussed further in our submission.

The AIIA submits that further guidance, clarity on the scheme's remit and reach as well as oversight mechanisms are required to ensure both industry support as the regime is implemented and that the scheme is fit for purpose and achieves the government's stated ambitions.

Cross-border data considerations and *Systems of Critical Infrastructure* (2018) Act Issues

The AIIA questions the geographical boundary of the *Systems of Critical Infrastructure* (2018) regime when it comes to IT and data; data may be stored in Australia but be replicated in other regions. Data does move between borders and is the basis of cloud and other ICT infrastructure and software business models. Therefore, a government entry onto Australian premises may have a downstream effect overseas, raising questions about international legal liability and impact on interconnected businesses.

The AIIA is strongly recommending that the Ministerial authorisation power includes an explicitly articulated obligation on the government to consider the supply-chain impacts before exercising its power to intervene in addition to positive obligation for decision-makers to consider existing regulatory systems imposing obligations on responsible entities, the costs likely to be incurred by responsible entities in complying with rules, the reasonableness and proportionality of the requirements and any such matters as the Minister considers relevant.

This could be inserted as an amendment to S35AB in the form of a replacement of ss(8)(c) (with the existing ss(8)(c) becoming ss(8)(d)):

> *[In determining whether the specified direction is a proportionate 25 response to the incident, the Minister must have regard to…*]
> *(c) the consequences of compliance on relevant supply chains*

As above, if the government were to direct or intervene with a cloud infrastructure provider, this could have material downstream implications across the whole supply chain without the knowledge of the SaaS, PaaS or CI customer.

Given the potential complexity of a cyber incident and the inter-relationship across the supply chain and the global connected environments of many cloud businesses, we recommend a holistic approach is taken. Where the government seeks to exercise the power

there is engagement across the digital supply chain in the event of a direction to act, or direct intervention.

Finally, in relation to access to system information, the AIIA suggests a comprehensive assessment of relevant international laws, for example the European Union's General Data Protection Regulation, be undertaken in order to understand whether the proposed legislation would have the potential to put entities in conflict with international obligations.

Specific definitional issues

The AIIA is pleased that the government has taken into account industry feedback regarding the definition of the data processing and storage sector, following from the initial use of the term 'data and the cloud'.

We also acknowledge the government's removal of the word 'commercial' from the definition of the data storage and processing sector.

The AIIA continues to posit that the sectoral definition for 'data processing and storage' and the scope for this sector is unclear, especially given 'data processing service' in section 5 is undefined. The AIIA continues to query what "relates to business-critical data" means in this context. For example, is it the intent that a cyber security product delivered via the cloud that, *inter alia*, protects an entity's business critical data would 'relate' to business-critical data? The Committee should also study the effects of the forthcoming *Privacy Act 1988* review, which is contemplating an expansion of the term 'personal information' to include IP addresses and other technical data, on the proposed definition in this bill of 'business-critical data'.

Regarding the definition of the sector, the AIIA also suggests that the same definition for 'business critical data' be applied to government workloads, just as it will to the private sector and other critical industries asset verticals, given government is a large threat vector.

Just as the government expanded and clarified the definition of the 'data storage and processing sector' to include all entities providing data storage or processing services, regardless of whether such services are provided on a commercial basis, a similar amendment should be made to the definition of 'critical data storage or processing assets' ensuring that all information technology providers are treated uniformly when it comes to attracting positive security obligations, whether a critical infrastructure entity manages, processes, hosts or stores data in the public cloud, in data-centres, or on-premise within its own data centres.

The criteria and rules prescribing what constitutes or designates critical assets or systems of national significance should be subject to periodic review, and entities should be able to trigger reviews by request of the government.

'Critical Cyber Security Incident'

The AIIA submits that Critical Cyber Security Incident reporting and other reporting obligations should explicitly be made to apply to incidents taking place within Australia and its territories only. The definition and criteria for a "critical cyber security incident" is not defined in the legislation. Of note, the term "significant impact" in section 30BC(1)(b)(ii) is not

defined. The Explanatory Document provides some commentary on this at paragraph 319, noting that determining whether an incident is having a significant impact on the availability of the asset will be a "matter of judgment for the responsible entity" and that the threshold has been left "intentionally undefined as the significance of an impact on the availability of an asset will vary radically between assets". It also notes that it is "not intended that day-to-day incidents ... should be reported." While this guidance is helpful, it does leave many organisations guessing what constitutes a "significant impact" on the availability of an asset. We would recommend that the Government take this as a focus for the co-design process.

'Other Cyber Security Incidents'

The threshold for reporting "other cyber security incidents" appears to be too low and the outcome of this provision will likely be an overreporting to the Commonwealth of incidents that may or may not be helpful.

Of note, Section 30BD(1)(b) sees the introduction of the requirement to report where a cyber security incident is not only where an incident has occurred, or is occurring but also, where a cyber security incident is "imminent". The term "imminent" is not defined in the Bill or the Explanatory Document. For example, does this refer to a scenario where there is a disclosed vulnerability, but the organisation is in the process of patching their systems? Does this require companies to report on attempted incidents? If so, this could see the Commonwealth burdened with thousands of reports per day.

The Bill also notes that the incident must have also "had, is having or is likely to have a relevant impact on the asset". It is unclear how a CI asset can determine whether an incident is likely to have a relevant impact - as 'likely' remains undefined and guidance on the parameters here is missing.

The AIIA suggests that 'Other Cyber Security Incidents' be reported by relevant entities as part of the annual reports, with the yearly reviews serving as an opportunity to consider whether notifiable 'Other' incidents should be categorised as 'Critical' incidents. Otherwise, industry and government run the risk of becoming overwhelmed by notifications of 'Other' cyber security incidents.

The Explanatory Memorandum goes further and explains that "by contrast to a critical cyber security incident, this obligation relates to any impact on availability (irrespective of significantly) alongside other forms of impact".

Reading section 30BD as whole, the reporting threshold is too low and will likely result in the Commonwealth being overwhelmed by reporting of cyber incidents – undermining their ability to provide timely and actionable advice to critical infrastructure assets.

Concerns regarding Part 2B - Notification of Cyber Security Incidents

The AIIA continues to hold the view that the respective timelines of 12-hours and 24-hours for reporting a "Critical Cyber Security Incident" and "Other Cyber Security Incidents" are unnecessarily short. This requirement injects additional complexity at a time when critical infrastructure entities are faced with the difficult task of responding to a cyber incident. It also greatly increases the likelihood that the CI entity will report inaccurate or inadequately

contextualised information that could be shared with the government and other members of industry. We recommend that the Committee consider whether these timelines should be replaced with a requirement for companies to report "as soon as reasonably practicable" or that each sector is subject to tailored timeframes decided in the co-design process. We also note that the full extent and impact of a cyber security incident may not be known or well understood within 12 hours of it being realised. Therefore, it may also be difficult for an organisation to determine whether it is a "critical" or "other" cyber security incident within the timeframes.

The AIIA supports concerns that we understand the Australian Banking Association (ABA) will be raising in its submission related to regulatory duplication and related compliance burden of two schemes (APRA and the CI regime) including consistency of reporting obligations, as reporting under APRA is required within 72 hours, not 12 or 24 as proposed in this legislation. This will likely apply to a number of other sectors with competing rules or regulations. The AIIA calls upon government to harmonise the timeframes within the legislation with these similar reporting regimes and amend the timeframe to 72 hours.

Obligations to consider supply chain and regulatory obligations

The AIIA is pleased by the government's amendments creating a positive obligation for decision-makers to consider existing regulatory systems imposing obligations on responsible entities, the costs likely to be incurred by responsible entities in complying with rules, the reasonableness and proportionality of the requirements and any such matters as the Minister considers relevant, which the AIIA posits could include the active obligation to consider effects on global supply chains and businesses operating over multiple countries.

The AIIA calls on the Committee in its review of the legislation to recognise and take into account often globally interconnected entities' obligations to maintain their intellectual property, manage commercial secrets and protect themselves against commercial risk.

In light of the AIIA's stated concern regarding the way in which the regulations and requirements would intersect with existing regimes affecting highly regulated sectors such as banking, energy and telecommunications, the AIIA also welcomes the new subsection (b) under s30CU Requirement to undertake vulnerability assessment, requiring the Secretary to consult relevant Commonwealth regulators that have existing functions relating to the security of the relevant critical infrastructure system. The AIIA has stressed the importance of avoiding regulatory duplication and over-regulation.

Consultation on rules and timeframes for review

The AIIA acknowledges the government's extension of time for submissions to be made in relation to rules that are published on the Department's website under section ABA – Rules from 14 days to 28 days. The AIIA is also pleased to see the addition of new section 30BBA Consultation—rules, stipulating that before making or amending rules, the Minister must publish the draft rules or amendments on the Department's website for a period of 28 days for the purpose of submissions, give a copy of the notice to each First Minister, and consider any submissions received within the 28-day period.

Ministerial authorisations, intervention requests and actions

A number of AIIA members believe that the data processing and storage sector should be exempt from the direct action provisions in the legislation and wish to find an alternative path to achieving the desired assistance outcomes with government for this sector. Others have expressed greater regulatory oversight and responsibility from government for cyber security incident management and reporting, but with the maximum clarity, consistency and opportunities for recourse and review.

In relation to s35AB, which relates to Ministerial authorisations, intervention requests and actions in the case of a cyber security incident, the AIIA posits that genuine disagreements as to strategy and best course of action ("*reasonable steps*") may arise between government and industry heads, that this may be interpreted for the sake of justifying intervention as an 'unwillingness' to take 'all reasonable steps to resolve the incident'. These concerns apply equally to s35AB(10), pertaining to ministerial intervention requests.

Therefore, the AIIA continues to believe that where a decision is made to issue a written notice or direction, the legislation should provide for the entity's ability to formally request the decision-maker to reconsider.

The 'technical feasibility', 'unwillingness' or 'inability' to take reasonable steps should be subject to an independent assessment that can be triggered by the appeal of the entity in question, should that entity believe in good faith that the entity possesses the willingness and ability to address cyber threats, but disagrees with the government's intended risk-mitigation strategy or course of action.

The AIIA maintains its contention that the Attorney-General would be more appropriate to include in the tri-Minister authorisation meetings rather than the Defence Minister, given the fact that the Attorney-General would have regard to legal and constitutional issues relating to direct intervention. If the Committee considers that the existing constitution of the meetings as including the Prime Minister, the Minister for Home Affairs and the Defence Minister, the AIIA submits that the Attorney-General and the Minister with responsibility for ICT and the Digital Economy be included in these meetings so that legal and industry issues are considered as part of these authorisations.

It is proposed that the independent appeals board be stood up on an on-call standby basis, and thus stood up when the Minister for Home Affairs convenes the tri-Minister meetings to authorise directions, with a review of membership between industry and government annually. Given the national security significance of acting quickly, the appeals process would only start a 12-hour 'clock' so that if action is indeed warranted, it would not be unduly delayed. Mechanisms for defined post-event review, potentially involving the same members of the board, should also be established. Given that the direct government intervention powers granted by Parliament to the SOCI Act over two years ago have never been used, this ask is proportionate given its likely rare use.

Operators must be notified that a direction is imminent and be given the opportunity to mount a defence, if required, before the direction takes effect, by being given a trigger for real-time review by a panel of independent arbiters or experts.

The legislation should also outline a process whereby a regulated entity may seek review by a judicial officer of the merits of the Government's use of 'assistance powers'. The stipulated

ability to refer contentious cases of governmental intervention to the judicial arm of government is essential in ensuring respect for the rule of law and appropriate recourse for regulated entities across so many sectors.

The action directions regime provides protections for entities, but in the case of the intervention direction regime, only the ASD is provided protection from liability. The government should provide protection from liability for entities subject to relevant directions.

Risk management program and sector-specific rules

The AIIA notes that we are unable to comment on hypothetical sector-specific rules prior to their publication. It is difficult for the AIIA to assess the regime as a whole without access to those rules and their method of formulation. It is important that co-design processes be rigorous and genuine.

The wording in s30AH as to sector-specific rules under the critical infrastructure risk management program is couched in the terms 'the rules *may* provide' [our emphasis], meaning that it is difficult to offer certain feedback in relation to these future rules.

We welcome the good faith provision in s30BE(1) regarding entities not being liable for actions or omissions done in good faith.

The AIIA suggests that the government consider extending the current forecast for rules coming into force from mid-year 2021 to end-of-year 2021.

The proposed legislation should give greater regard to harmonisation with international standards and certification regimes, including the ISO 27000 series, with many global providers already meeting these certification standards.

Red tape and regulatory burden; potential for duplication

The AIIA acknowledges the importance of having cyber security frameworks in place for entities and assets of national significance. However it must be noted that the proliferation of regulatory requirements – such as to undertake vulnerability assessments, cyber security exercises, the preparation of periodic reports for the Secretary (s30DB), and event-based reporting (s30DC) – are of concern to the AIIA's members for their cumulative regulatory impost on industry, which in Australia has fulfilled a gold standard of cyber security management to date.

For the exercises and assessments an entity is required to undertake, the AIIA submits that a cap on the number of times an entity may be asked to participate, and that reports should be made available if actively requested by government on an as-needs basis, but not automatically required wholesale across the sector. The latter would constitute an unnecessary administrative and red tape burden on affected entities.

Conclusion

The AIIA is supportive of bolstering cybersecurity across the economy, but remains concerned about unnecessary increased regulatory burdens, such as positive reporting requirements, as well as the expansion of executive powers of intervention.

The AIIA supports the government imposing a regime that acknowledges the importance of cybersecurity and cyber resilience to building trust in the imperviousness of critical Australian infrastructure to debilitating attacks and incursions. Government must also accept that any heavily regulated sector with related compliance costs and substantial obligations borne by industry in itself sends a strong market signal that drives investments accordingly for those cloud and other sectors.

We are ready to work with government in the co-design of flexible, proportionate sectoral-specific rules and to iron out any unintended consequences of the regime for government and industry as we seek to cooperate in the implementation of these reforms. We thank government for their amendments to the Bill and thank the Committee for considering the specific implementational issues raised by this submission.

We would welcome a further opportunity to engage with government on this legislation. Should you have any questions about the content of this submission, please contact policy@aiia.com.au.

Yours sincerely,

[redacted]

Simon Bush
GM, Policy and Advocacy
AIIA