aiia
australian information
industry association

AUSTRALIAN INFORMATION INDUSTRY ASSOCIATION

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Submission to the Department of Home Affairs

30th November 2020

Contents

Summary of recommendations 3

Introduction 5

Retained concerns regarding rush to legislate 5

Specific definitional concerns 6

Concerns regarding Part 2B - Notification of Cyber Security Incidents 7

Timeframes for Cyber Security Reporting 7

'Critical Cyber Security Incident' 7

'Other Cyber Security Incidents' 7

Obligations to consider digital supply chain and international obligations 8

Ministerial authorisations, intervention requests and actions 9

Risk management program and sector-specific rules 11

Red tape and regulatory burden; potential for duplication 11

System information software notice 12

The Singapore example; little precedent for extensive direct action powers 12

Conclusion 13

Summary of Recommendations

That the government:

- Consider the appropriateness of direct intervention powers for the data storage and/or processing sector.
- Draft rules for the data processing and/or storage sector subsequent to other sector regulations
- Ensure the data processing and/or storage sector is only subject to rules that are genuinely co-designed.
- Engage in further industry consultation regarding oversight, sector-specific rules and the application of new laws to existing regulated sectors such as banking, energy and telecommunications.
- Reconsider the inclusion of the 'commercial' criterion in the definition of the data storage or processing sector.
- Clarify the definition of activities 'relating to business-critical data'.
- Consider the effects of the forthcoming *Privacy Act 1988* review and its contemplated expansion of the definition of 'personal information' on the definition of business-critical data.
- Apply the same definition for 'business critical data' to government workloads.
- Make the criteria and rules prescribing the constitution or designation of critical assets of systems of national significance (SoNS) subject to periodic review and requests by entities for review.
- Replace the 12- and 24-hour timelines for "Critical Cyber Security Incidents" and "Other Cyber Security Incidents" with tailored sector-specific timeframes in consultation with industry.
- Make reporting timeframes harmonious with existing regulations on regulated sectors such as banking
- Define "critical cyber security incident" and "significant impact" and make these definitions a focus of the co-design process with industry.
- Increase the threshold for reporting "other cyber security incidents.
- Define the term "imminent" in section 30BD(1)(b) and the term "likely to have" in relation to other cyber security incidents and impacts on the asset.
- Include as part of the Ministerial authorisation power an obligation to consider the supply-chain impact globally before exercising its power of intervention, in the form of a substitution of a replacement of ss(8)(c) (with the existing ss(8)(c) becoming ss(8)(d)) as follows:
    - *(c) the consequences of compliance on relevant supply chains*
- Undertake a comprehensive assessment of relevant international laws, e.g. the EU's GDPR, to understand the proposed legislation's potential to put entities in conflict with international obligations.
- Provide for the entity's ability to formally request the relevant decision-maker reconsider (in the case of ministerial authorisations, intervention requests and actions).

- Provide for real-time recourse to an independent board, in the form of an eighteenth section under s35AB (mirrored elsewhere in the legislation as relevant):
    - *Ministerial discretion subject to entity's right to appeal to independent board*

      (18) If the entity subject to the ministerial authorisation or intervention request disagrees with the directions or requests made under 35AB(2) or (10) in relation to a critical infrastructure asset, the entity may have recourse to an independent critical infrastructure appeals board comprised of an adjudicator, that being a former federal judicial officer, and a mutually agreed industry appointee with the requisite expertise in cyber security management, upon which time a 12 hour injunction will take effect until the independent appeals board has made a declaration as to the reasonableness and justification of the Ministerial authorisation or direction.
- Stand up an independent appeals board on an on-call standby basis, to be convened in parallel to the tri-Minister meetings to authorise interventions, actions, and so forth, with the board to be made up of a former judicial member and independent cybersecurity expert/s.
- Substitute the Attorney-General for the Defence Minister in the aforementioned tri-Minister meetings.
- Provide for the notification of operators when a direction is imminent to give the opportunity to mount a defence and trigger real-time review by the independent appeals board.
- Provide protection from liability for entities subject to relevant directions.
- Put the legislative process on hold while sector-specific rules are drafted to allow for the minimisation of regulatory impacts, duplication, conflicts and contradictions.
- Consider extending the current forecast for rules coming into force from mid-year 2021 to end-of-year 2021.
- Introduce a cap on the number of times an entity may be asked to participate in exercises and assessments.
- Make the availability of routine reports subject to an as-needs basis or request from the government.
- Contemplate an entity's compliance with written notices and directions where it would run counter to commercial contracts or company constitutions, as with s11CD and 14AA of the *Banking Act.*
- Remove the ability for government to mandate a specific software installation (s30DJ(2)).
- Exclude the data storage and processing sector from exposure to mandatory software installation if the power is to persist.
- Put additional safeguards and frameworks in place around the installation of the software, such as assessment by the entity's security teams, if no exclusion is to be granted.

Introduction

The AIIA supports the expansion of industries that are defined in this bill as critical industries (**CI**) and fall under this regulatory scheme. This review of critical industries and infrastructure and the preceding consultation paper recognises 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.

While the draft legislative framework is intended to render assistance to operators, including by preventing imminent cyber security incidents (12P(a)), mitigating the relevant impact of said incidents on critical infrastructure assets (12P(b)) and restoring functionality to such assets (12P(c)), we do question the appropriateness and application of powers inherent in the legislation for the data storage or processing sector, given its complexity, interconnectedness, overlapping regulatory regimes and the potential global implications.

The government should give consideration to whether the direct intervention powers in the legislation are appropriate for this sector, as the sector already has a high level of cybersecurity capability, with a large portion of the sector already complying with positive reporting obligations related to cyber incidents and threats as a result of their IRAP and protected cloud status through ACSC and the workloads it supports for government. If the intent of this legislation is to capture less mature entities in this sector, the legislation has no mechanisms sensitive to that distinction. Furthermore, these entities are often globally connected to supply chains, so these impacts are naturally of great concern to our members.

The government should ensure the sector is only subject to rules that are genuinely co-designed and flexible and consider drafting the rules for this sector subsequent to other sector regulations to ensure there is no duplication and that all relevant gaps are filled.

Regarding the direct action power against the data and processing sector, the AIIA suggests, at a minimum, that the government ensures appropriate appeal mechanisms, the opportunity for injunction and the contemplation of an independent expert panel if such powers are to be provided for in the Act.

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

Retained concerns regarding speed to legislate

The AIIA remains concerned that an important and critical area of policy is being rushed through to legislation when industry has significant questions around the detail, scope and remit of the proposed expansion as well as the operation of new direct action powers and avenues for recourse. We believe further industry consultation is required, especially in relation to oversight and sector-specific rules as well as understanding how the new laws relate to other regulated sectors like banking, energy and telecommunications.

Whilst acknowledging that the government has listened to industry concerns around the process by releasing an Exposure Draft prior to being introduced to parliament and that in response to initial feedback the government has sought to bolster oversight arrangements, and stipulated that powers may only be enlivened in scenarios of genuine national emergency, we still harbour concerns around the breadth, speed, definitions and sector-specific thresholds that have been embedded into the legislation.

Although the AIIA has a fundamental concern with the extensive nature of the direct action power itself, in view of the Government's resolve to legislate in this area and the short timeframe before introduction to parliament, the AIIA is focusing this submission on said oversight arrangements and avenues for real-time recourse.

Specific definitional concerns

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'.

While the AIIA appreciates that the definition has been developed in this direction, we would query the embedding in the definition of the word 'commercial':

> *data storage or processing sector means the sector of the 25 Australian economy that involves providing data storage or 26 processing services on a commercial basis.*

The government should consider whether making the commercial nature of data storage or processing a prerequisite for inclusion in this regime could lead to unintended consequences. If an entity processes or stores data as its primary function but could argue that it does so on a non-commercial or not-for-profit basis, but otherwise meets the criteria for operating systems of national significance or owning critical assets, the AIIA would query whether such entities should be considered to exist outside of the data storage and processing sector.

The AIIA queries the sectoral definition for 'data processing and storage' and believes the scope for this sector is unclear, especially given 'data processing service' in section 5 is undefined. The AIIA would 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 government 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.

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.

Concerns regarding Part 2B - Notification of Cyber Security Incidents

We note the importance of sharing information about cyber security incidents to prevent and minimise the impact of future cyber security incidents on others. We also welcome a notification system that takes into account the significance of the incident. However, we have the following observations:

Timeframes for Cyber Security Reporting

The timelines of 12-hours and 24-hours for reporting a "Critical Cyber Security Incident" and "Other Cyber Security Incidents", respectively, 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 strongly recommend that the Government replace these timelines 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.

'Critical Cyber Security Incident'

The AIIA submits that this 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 Explanatory Document 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.

Obligations to consider digital supply chain and international obligations

In section (8) it is specified that *"… in determining whether the specified direction is … proportionate … the Minister must have regard to … the impact of the specific direction on … the activities carried on by the specific entity … and … functioning of the asset concerned."*

The AIIA remains concerned that the proposed Ministerial Authorisations for cyber security incidents focuses the engagement solely upon a 'relevant entity".

Cyber threats to CI may arise at different parts of the digital supply chain but have implications across the whole supply chain and for global cloud providers be they platforms (IaaS) or software (SaaS) they are often globally interconnected so naturally these providers are very sensitive about any direct action occurring in Australia that affects its global business.

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 can move between borders. Therefore, a government entry onto Australian premises may have a downstream effect overseas, raising questions about international legal liability.

Furthermore, 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.

We therefore recommend that the Ministerial authorisation power includes an obligation on the government to consider the supply-chain impacts before exercising its power to intervene.

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*

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.

<u>Ministerial authorisations, intervention requests and actions</u>

A significant portion of AIIA's represented entities 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 crave 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.

Under s35AB, which relates to Ministerial authorisations, intervention requests and actions in the case of a cyber security incident, it is stipulated that:

> *(7) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) unless the Minister is satisfied that:*
> *(a) the specific entity is unwilling or unable to take all reasonable steps to resolve the incident; and*
> *(b) the specified direction is reasonably necessary for the purposes of responding to the incident; and*
> *(d) compliance with the specified direction is technically feasible.*

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 believes 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 proposes that the government insert an eighteenth section under s35AB:

> *Ministerial discretion subject to entity's right to appeal to independent board*
>
> *(18) If the entity subject to the ministerial authorisation or intervention request disagrees with the directions or requests made under 35AB(2) or (10) in relation to a critical infrastructure asset, the entity may have recourse to an independent critical infrastructure appeals board comprised of an adjudicator, that being a former federal judicial officer, and a mutually agreed industry appointee with the requisite expertise in cyber security management, upon which time a 12 hour injunction will take effect until the independent appeals board has made a declaration as to the reasonableness and justification of the Ministerial authorisation or direction.*

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.

Regarding the tri-Minister meetings, which consist of the Prime Minister, the Minister for Home Affairs, and the Defence Minister, the AIIA submits that as the Defence Minister would, it is fair to assume given his or her defence focus, naturally lean on the side of intervention in response to national security threats, that the Government give consideration to either including, or substituting in place of the Defence Minister, the Attorney-General in this convened meeting. This, we argue, would bolster the rigour and credibility of this layer of approval and afford genuine legal and constitutional *nous* to the oversight process inherent in the legislation and remove the Defence Minister's role in approving a domestic enforcement action.

The AIIA notes that the Department of Home Affairs, in a briefing to the AIIA on the Consultation Paper, when the AIIA posed the question regarding whether the Defence

Minister was required to approve a Secretary of Home Affairs request for an Australian Cyber Security Centre (ACSC) intervention, answered in the negative. In other words, there is no legal or process reason, the AIIA was told, for the Defence Minister's involvement.

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 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 AIIA suggests that the legislative process be put on hold while sector-specific rules are drafted so that the framework may be considered globally for regulatory impacts and to minimise duplication, conflicts and contradictions across the system.

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.

The AIIA further understands that there are legitimate concerns around how the regulations and requirements would intersect with existing regimes affecting highly regulated sectors such as banking, energy and telecommunications, with a potential for duplication and confusion. In fact, on 26th November, media reported that APRA intends to expand its regulatory approach, breadth and scope in relation to cyber security and reporting including software[1].

The legislation may need to contemplate an entity's compliance with written notices and directions when such compliance would run counter to the content of relevant commercial contracts or the company's constitutions. There are models for dealing with these issues in preceding legislation, such as the *Banking Act* (section 11CC).

Any elements of overreach in this regime may indeed have a cascading effect economically; with the perception of undue regulatory burden and executive overreach in respect of the functioning of the direct action powers, the CI regime as it stands may impact investment decisions affecting Australia and its assets.

<u>System information software notice</u>

The requirement that under certain circumstances entities install a specific computer program on their computers (s30DJ(2)) – with a requirement in the latter case to 'consult' but no further recourse (s30DK) and a civil penalty equating to 200 units (s30DM) if the entity fails to comply with the system information software notice is greatly concerning to the AIIA and constitutes extraordinary overreach. The mandatory installation of government-selected software in any entity's systems on pain of civil penalty is troubling in itself, but the potential impacts on global interconnected businesses such as cloud providers is of particular concern.

The AIIA submits that the data storage and processing sector be excluded from exposure to system information software notices if this power is to persist in the legislation. At the least, additional safeguards and frameworks ought to be put in place, such as the entity's security teams being able to undertake an assessment of the software and an ability to seek an injunction.

The government ought also consider that if multiple critical infrastructure systems are required to install the same piece of government-mandated software, this itself can represent a vulnerability in the system.

<u>The Singapore example; little precedent for extensive direct action powers</u>

The AIIA notes that the Republic of Singapore's Critical Information Infrastructure ('CII') regime, enshrined in the *Cybersecurity Act 2018*, was significantly revised in response to industry feedback regarding impacts on the global supply chain and the threshold for critical

[1] https://www.afr.com/companies/financial-services/apra-warns-it-s-ready-to-prosecute-for-lax-cyber-security-20201126-p56i4t

cybersecurity incidents. Computer systems in the supply chain supporting the operation of a CII were not designated as CII, meaning that data centre owners and operators were not caught by the regime.

Notwithstanding Singapore's critical infrastructure regime, in the context of the five eyes of Australia, Canada, New Zealand, the United Kingdom and the United States of America, this extent of direct action power is unprecedented and government must, as a prime mover in this area, tread with caution and implement significant thresholds, definitional clarity and oversight measures.

Conclusion

The AIIA remains concerned by the direct-action power and its effect on global supply chains, even though there is a high threshold described the draft legislation and refined definitions. We remain concerned about the application of the power and the functional threshold for making authorisations and declarations. The industry wants confidence in an oversight process providing real-time recourse for the operator.

The AIIA is generally supportive of bolstering cybersecurity across the economy, but is concerned about regulatory burdens, such as positive reporting requirements, as well as legislative and executive overreach, which could impact on investment decisions.

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,

Simon Bush
GM, Policy and Advocacy
AIIA