Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

1 March 2022

REVIEW OF *THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022* – AIIA RESPONSE

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.

Some 92% of AIIA members are small and medium Australian businesses and 8% of AIIA members are large Australian companies and multinational corporations.

Introduction

The AIIA welcomes the opportunity to provide its response to the *Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*. The AIIA considers the basis for the implementation of a successful regulatory regime is for the Government to

collaborate with industry, so as to ensure that any such provisions satisfy mutual interests and, where appropriate, address deficits and concerns.

Accordingly, the AIIA initiated its response to this consultation mindful of the concerns of its members over the process that the Government has engaged in for the passage of the proposed Bill. Whilst the AIIA is cognisant of the need to address national security concerns, the hurried reviews of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and the proposed 2022 Bill, coupled with the lack of due consideration given to industry stakeholder interests, will be to the detriment of any regulatory regime the Government seeks to institute. It is the opinion of the AIIA that any legislation which will have as significant an impact on Australian economic and security interests should be subject to conscientious development, and be fully inclusive of all interests.

Organisations such as the AIIA devote substantial time and resources in engaging with Government to ensure its interests are represented, and are committed to continuing this activity for the foreseeable future. The AIIA strongly encourages the Government to continue to engage with relevant stakeholders so as to ensure that any such legislation is fit for purpose to ensure positive outcomes in the longer-term.

AIIA RESPONSE

Systems of National Significance

Under proposed Division 2 of Part 2A, the Bill states that the Minister may privately designate a critical infrastructure asset to be a System of National Significance (**SoNS**), enabling the Secretary of the Department of Home Affairs to direct that one or more cyber security activities be undertaken by the infrastructure owner.

Given the nature of this designation, it is recommended that the Department of Home Affairs consult directly with responsible entities prior to the Minister providing notice of a proposed SoNS declaration. This would provide companies with an opportunity to respond and provide accurate information on their assets directly to the Government.

Recommendation: That the Department of Home Affairs consult directly with responsible entities prior to the Minister issuing notice of any proposed SoNS declaration.

Under proposed section 52C (Consultation – declaration), the proposed consultation period is currently designated as 28 days or less. The Minister for Home Affairs may also determine whether a shorter response period should be imposed if the circumstances are deemed sufficiently urgent.

The AIIA believes the proposed consultation period will place an unnecessary administrative burden on any company requested to provide a response. The Government must give due consideration to the impact such requests will impose on companies, which is not sufficiently covered in the proposed Bill.

Given the processes that will first need to be satisfied before an entity will be in a position to provide its response, the current timeframe is too brief. The AIIA recommends the consultation

period for entities be extended to 40 days at minimum, with provision to extend the response time on a case-by-case basis.

Recommendation: That the consultation period for SoNS-declared entities to provide a response to the Minister for Home Affairs is extended to 40 days, with provision to extend the response time on a case-by-case basis.

To alleviate any potential administrative burden, the AIIA recommends the Bill be amended to specify that any Ministerial request to provide a comprehensive outline of any critical information required to be submitted as part of a response. This will provide entities with sufficient information to determine whether it is in a position to respond to the Ministerial request.

Recommendation: That any Ministerial request is inclusive of a comprehensive outline of any critical information to be submitted by an SoNS-declared entity.

In defining the scope of what constitutes an SoNS, the AIIA recommends that the Bill exclude operating systems for desktop and mobile technology hardware such as smartphones and tablets. Specific examples include Windows, iOS for Mac, Google Android and Apple iOS operating systems. The inclusion of such operating systems presents an additional level of complexity to the proposed SoNS system, as systems which are developed with an international user base would be unable to function in domestic market subject to such access provisions.

Recommendation: That operating systems for desktop and mobile technology hardware, such as Google Android and Apple iOS are not included as SoNS entities.

Protected information

Under section 52B of the Bill, an asset is declared to be an SoNS within the definition of protected information. Under these conditions, an SoNS-declared entity is prevented from disclosing to third parties that they have received such a designation.

The AIIA recommends that the Bill, or alternatively the Explanatory Note, be amended to permit entities to disclose SoNS declarations of assets (subject to relevant confidentiality agreements etc.) to a limited number of third parties.

Such a measure would provide appropriate protection to SoNS-declared entities and prioritise company assets and activities. While disclosure may be required in order to comply with the Act, this may also arise as part of standard business operations and should be permitted subject to applicable confidentiality requirements.

Recommendation: That the Bill, or alternatively the Explanatory Note, be amended to permit entities to disclose SoNS declarations of assets (subject to relevant confidentiality agreements etc.) to a limited number of third parties.

Due to the nature of the proposed amendments, in that Government agencies would have access to highly sensitive materials and information, the AIIA recommends that the Bill be inclusive of a provision whereby information sharing is confined to relevant Government departments (i.e., Department of Home Affairs, intelligence agencies, etc). Any agency seeking to access information received by the Government under the SoNS provisions must be subject to Ministerial approval and the relevant SoNS-declared entity should be informed of any such request prior to Ministerial approval.

Recommendation: That the Bill include a provision confining information sharing of any materials received from SoNS-declared entities to relevant Government departments, with any external departmental requests subject to Ministerial approval and informing of relevant SoNS-declared entities.

Critical infrastructure risk management program

Under proposed section 30AH (Critical infrastructure risk management program), critical infrastructure stakeholders are required to identify and take all reasonable steps to mitigate all hazards across cyber, supply chain and physical operations.

The AIIA considers the proposed introduction of Risk Management Plans to be a key pillar of the Government's critical infrastructure reforms. Risk management in this context has the ability to create real and meaningful cyber security uplift across the Australian economy and in turn foster a culture of cyber security.

The AIIA acknowledges the efforts of the Government in engaging with industry in the development of the Risk Management Plans - Program Rules. These rules have been subject to revision via the industry consultation process and these are now satisfy the respective interests of both Government and the Australian ICT industry.

The Explanatory Memoranda to the Bill states the Critical infrastructure risk management program obligations would have a minimum six month delayed implementation, to allow relevant business practices to be aligned. The AIIA notes that, by including the six month provision in the Explanatory Memoranda, the Government makes an explicit commitment to ensuring the delayed implementation of the Critical infrastructure risk management program included in the Bill.

Enhanced Cyber Security Obligations

The Explanatory Note states that enhanced cyber security obligations will be considered on a case-by-case basis, following consultation with individual SoNS entities.

Under these conditions, the AIIA recommends that the Bill be amended to include a provision whereby the Secretary would consult with entities before applying any enhanced cyber security obligations under Part 2C.

Additionally, either the Bill or Explanatory Notes should include the decision-making criteria by which the Secretary must adhere to prior to submitting a request to a designated-SoNS entity to comply with the enhanced cyber security obligations.

Recommendation: That the Bill be amended to include a provision whereby the Secretary would consult with entities before applying any enhanced cyber security obligations under Part 2C

Recommendation: That either the Bill or Explanatory Notes include the decision-making criteria by which the Secretary must adhere to prior to submitting a request to a designated-SoNS entity to comply with the enhanced cyber security obligations.

Right of Appeal

The AIIA recommends that the Bill include provision for a merits-based review for any decision made its auspices. Given the broad nature of these powers, it is critical that SoNS-declared entities have recourse to an appeal mechanism should there be any dispute with a decision concerning information requests or any related issue. The absence of such a review mechanism may have an adverse impact on the Australian ICT sector and international perceptions of the Australian business environment.

Recommendation: That the Bill include an appeal mechanism to enable any SoNS-declared entity to address any disputes or related issues relating to information requests.

Access to System Information

Under the terms of the proposed Bill, the Secretary may request the owner of any SoNS-designated asset to provide what is broadly termed "systems information" to the Department of Home Affairs. The AIIA notes that whilst personal information as defined under the *Privacy Act 1988* would not be subject to this provision, these requirements may potentially include real-time or periodic reporting.

The proposed Bill states under section 30DC(4) that the Secretary is required to take into due consideration any costs that may be incurred by an entity in complying with a request and to consult with any entity prior to issuing a request under section 30DD, there is currently no provision in the Bill for an independent oversight mechanism to assess the validity of any such action. The AIIA recommends that an independent oversight mechanism administered under the jurisdiction of the Department of the Attorney-General be incorporated into the Bill, so as to assess any such request on their merits prior to submission to SoNS asset owners.

Additionally, due to the potential administrative and financial burden that an entity may incur as a direct consequence of receiving such a request, the AIIA recommends that the Bill institute a mechanism to enable entities to recoup costs (either in part or in full).

The AIIA is of the opinion that neither the Government or the Department of Home Affairs has provided adequate justification for the inclusion of this provision in the Bill, nor sufficiently articulated how or under what conditions this software would be used. The AIIA considers the inclusion of such provision to be a major legislative overreach and not a feature of a liberal democratic government. We encourage Members of Parliament and current members of the PJCIS to question the necessity and justification for such powers and whether such a provision is warranted.

Recommendation: That provision for an independent oversight mechanism administered under the jurisdiction of the Department of the Attorney-General be incorporated into the Bill to assess requests for access to system information prior to submission to SoNS asset owners.

Recommendation: That the Bill institute a mechanism to enable entities to recoup costs (either in part or in full) incurred as a direct consequence of receiving requests for access to system information.

Installation of Monitoring Software

Section 30DJ of the proposed Bill states the Secretary may require an entity responsible for an SoNS to both install and maintain a specified computer program to collect and record system information to be transmitted to the Australian Signals Directorate.

The AIIA considers such a provision to be overtly intrusive and strongly recommends this be removed from the Bill in full.

The installation of what is constituted third-party software has the potential to create vulnerabilities which would adversely impact SoNS assets as well as, by default, Government systems and client systems.

Additionally, the mandatory provision for installation of government software has the potential to adversely affect entity business interests, as clients may doubt system integrity for Australian-based ICT companies and opt to instead pursue off-shore ICT service providers.

The AIIA is of the opinion that neither the Government or the Department of Home Affairs has provided adequate justification for the inclusion of this provision in the Bill, nor sufficiently articulated how or under what conditions this software would be used. The AIIA considers the inclusion of such provision to be a major legislative overreach and not a feature of a liberal democratic government.

We encourage Members of Parliament and current members of the PJCIS to question the necessity and justification for such powers and whether such a provision is warranted.

Recommendation: That Section 30DJ of the proposed Bill be removed in full.

Closing Remarks

In closing, the AIIA recommends that following the passage of the final Bill that any resulting legislation is subject to biannual statutory review. This will ensure that any measures instituted by the Bill are robust and will in turn determine whether those parties subject to the ensuing regulatory framework are able to meet these requirements.

Additionally, given the nature of the proposed Bill, the AIIA recommends that the Government give due consideration to developing operational guidance materials to support industry in meeting any legal requirements. The AIIA would welcome an opportunity to act as a facilitator between Government and the Australian ICT industry in the development of any materials. These may include, but are not confined to, guidance on cyber incident reporting or development of risk management plans.

Thank you for considering this response. Should you have any enquiries about the content of this submission, please contact policy@aiia.com.au.

Yours sincerely,

Simon Bush
GM Policy and Advocacy, AIIA