aiia
australian information
industry association

AIIA Submission to

Strengthening Australia's cyber security regulations and incentives Discussion Paper Consultation

27 August 2021

aiia
australian information
industry association

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 the end-to-end digital ecosystem in Australia, including:
• multinational companies
• large Australian technology, telecommunications and digital and cloud infrastructure companies; and
• a large number of small and medium businesses, start-ups, universities and digital incubators.

Introduction

The AIIA has been supportive of government efforts to up lift cyber security and resiliency across the economy and have supported the Department of Home Affairs critical industries co-design process for the data and processing sector and other defined critical industries to uplift cyber security across the economy.

After reforming the IRAP and government cruber requirements of industry and the CI process covering critical sectors of the economy, the Department of Home Affairs is now looking at the 'rest of the economy'. In doing so, the AIIA supports an incentive-driven approach to cybersecurity uplift those areas of the economy not captured under other government regulatory systems and international and Australian cyber standards. The AIIA would welcome the opportunity to work further with the Department of Home Affairs in encouraging this cyber security uplift given the expertise of our members in this area. What the government has not done is understand what parts of the economy are exposed following the CI legislation and reforms and where are the areas of concern outside these supply chains. We therefore urge government to conduct a gap analysis to ensure helpful and targeted government engagement in the wake of the implementation of the Critical Infrastructure reforms.

Market and industry-led approach to standards, certification and compliance

The AIIA supports the call of the IoTAA for a market-led approach to this issue as opposed to a mandatory government-led scheme for certification. A principles-based approach, given the broad and diverse spectrum of organisations that government is seeking to uplift, rather than a mandatory certification-based approach, will be best-suited to address true risk across the economy.

Standards Australia has undertaken significant work in the last three years on cyber security standards, with there being a number of strong international standards in this area, and recommended Australia play a greater role in the development and adoption of cyber security standards across the Pacific. The Department should ensure congruence with this important work.

Large enterprise, SMEs, and the public sector

The AIIA is of the view that acceleration in the uptake of cloud technology by small and medium enterprises (**SMEs**) will greatly assist in removing cyber security pain points and lead to the adoption of standardised best practices across industry.

The large software, cloud and ICT infrastructure providers have a robust set of frameworks that have cyber security controls baked into the service which support the business that operate vertically under these software or infrastructure platforms. Creating incentives for large enterprises to assist SMEs in implementing best-practice standards will function as a rising tide of cyber security uplift that lifts all boats.

It is important that there not be unintended expectations created at the consumer level that using SMEs takes a risk with their data, but whole-of-economy uplift, large-enterprise and SME collaboration, and full leverage of cloud technologies is essential in this regard.

Cyber security hygiene

As referenced above, most large technology enterprises implement security-by-default, which is built into their design of systems, However, when breaches and issues do occur by customers, it is often the end-user taking either deliberate or unintended action in altering security controls or implementing poor cyber security hygiene (such as arise with weak, commonly-used or compromised passwords) often responsible for introduced weaknesses. The ACSC has acknowledged that most significant cyber security weaknesses are as a result of poor cyber knowledge, controls and behaviours and that education around cyber security hygiene and controls at the consumer level are essential.

Critical Infrastructure focus

Given the regulations being enacted across the economy with the significant Critical Infrastructure regime, which will put conditions on Australian supply chains including in respect of cyber security, government should focus on visible gaps rather than introducing a duplicative burden of codes, regulation and mandatory compliance when industry is focused on implementing massive changes resulting from the Critical Infrastructure legislation.

Clean Pipes Strategy

The AIIA notes that there is no reference to a Clean Pipes Strategy in the provided discussion paper.

As summarised by the Australian Strategic Policy Institute:

> *Clean Pipes could involve ISPs using a variety of technologies to provide default security to their clients. At the conceptual level, this would involve:*
>
> 1. *positively identifying threats, which could be, for example*
>   - *internet locations that host malware or phishing*
>   - *malware command and control*

   - *bogus traffic that can be used in attacks that try to overwhelm a service*
   - *'spoofed' traffic that claims to originate from somewhere it doesn't*
2. *having some capability to proactively protect from different threats, such as*
   - *blocking and warning users who are attempting to navigate to dangerous locations, such as ones that host malware or phishing*
   - *removing bogus or spoofed traffic*
3. *being able to adjust this blacklist dynamically and alter it through customer feedback if a location is inadvertently blacklisted.*[1]

Clean pipes has the advantage of affording scalable protection to the entire customer base of an ISP, whether SMEs or individual Australian citizens.

Given the reference by government to Telstra's Cleaner Pipes Initiative in the *Australia's Cyber Security Strategy 2020* document, and the fact that the CESAR package announced by government in June 2020 allocates more than $12m was allocated to a Clean Pipes-style initiative involving "new strategic mitigations and active disruption options, enabling ASD and Australia's major telecommunications providers to prevent malicious cyber activity from ever reaching millions of Australians across the country by blocking known malicious websites and computer viruses at speed," this is a curious omission.

Incentivising telecommunications providers to block cyber security threats in real time and at scale should be a priority focus of government as a sensical, industry-led means of targeting cyber security uplift.

Conclusion

As stated above, the AIIA would welcome further opportunities to partner with government in implementing incentive-based cyber security uplift across industry, leveraging the expertise of its members. Should you have any questions about the content of this submission, please contact [redacted].

Yours sincerely,

[redacted]

Simon Bush
GM, Policy and Advocacy
AIIA

[1] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet