Australian Information Industry Association

Response to the

Cyber Security Strategy 2023-2030 Discussion Paper

20 April 2023

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. 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 are unique in that we represent the diversity of the tech ecosystem from small and medium businesses, start-ups, universities and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies.

Introduction

The AIIA represents members for whom cyber security and custodianship of data are of the most serious priority. The AIIA also represents leaders in the cyber security industry across Australia and the globe. Finally, the AIIA represents members who are subject to the growing regulatory and legislative frameworks governing cyber security, data hosting and the reporting of cyber security incidents in Australia. It is these three equally important perspectives which ground our response to the *Cyber Security Strategy 2023-30* Discussion Paper.[1] The Government rightly has concerns around ensuring that Australia's economy is cyber-secure with the focus to date on Critical Infrastructure (CI) and Systems of National Significance (SoNS), which the AIIA has supported in the main.

Technology rightly underpins an increasing number of key national services and functions in Australia, with an increased exposure to cyber security threats an inevitable corollary alongside the immeasurable benefits provided. Furthermore, physical, personnel and cyber security are all increasingly interrelated, while cybercriminals and nation-state actors are growing increasingly sophisticated.

The 2022 European Union Agency for Cybersecurity (ENISA) Threat Landscape Report found that cyber security attacks "continued to increase during the second half of 2021 and 2022, not only in terms of vectors and numbers but also in terms of their impact."[2] Destabilisation in the geopolitical landscape, including with the Russia-Ukraine crisis, will see a paradigm characterised by cyber operations, state-sponsorship of cyberattacks and potentially the targeting of critical civilian infrastructure.2 Profitable cybercriminal groups have increased exponentially in size, targeting all industry segments indiscriminately, including Small and Medium Enterprises (SMEs), healthcare organisations and local, state and federal government systems. In the financial year 2021-22, the ACSC was in receipt of more than 76,000 cybercrime reports. This represents an uptick of almost 13 per cent from

[1] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[2] P.7, ENISA Threat Landscape 2022, November 2022

the 2020-21 financial year and equates to a report every 7 minutes, an increase from a report every 8 minutes year-on-year.[3]

The high-profile data breaches that took place in 2022 and 2023 have drawn an understandable focus from government and customers on how organisations ask individuals to prove their identity and then how long the organisation retains such data after the identity is verified. The AIIA welcomes the digital identity framework adoption by government's around the country. These breaches also show that there needs to be a careful balance in policy and regulator approaches and partnership between industry and government to ensure that businesses feel confident in informing regulators and their customers of a breach and seek help from government where it may be required.

The AIIA supports the vision, ambition and action-oriented features of the proposed Strategy. Understandably, when technology accelerates and digital platforms underpin the everyday existence of Australian citizens, and personal data is stored online, government will seek to ensure that the legislative and regulatory underpinnings are sufficient for Australians to have confidence about their personal information and security. The AIIA welcomes a strategic, streamlined and industry-collaborative approach to regulating privacy, data security and cyber security in Australia in line with community expectations. However, the Government has a number of regulatory and at times overlapping regimes with the new CI SoNs legislation and rules still yet to be fully implemented across the economy. We support the continued focus to ensure cyber resiliency across the economy and look forward to working with government to achieve this ambition.

The role of the Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD), the reporting requirements under the Notifiable Data Breaches Scheme as administered by the Office of the Australian Information Commissioner (OAIC) ,[4] the reporting available through *ReportCyber* via cyber.gov.au[5] and the legislative powers available under the Critical Infrastructure regime[6] are sufficient avenues for reporting and response, and together often give rise to a plurality of reporting mechanisms alongside non-government reporting requirements such as that pertaining to the ASX.[7] The AIIA believes that given some of the new rules and obligations have not yet taken effect across the economy, novel government regulation should be carefully considered and not hastened. The strategy should first consider how to enhance and build effective threat-sharing networks, threat-blocking activities, public-private partnerships and best-practice cyber security principles at both the organisational and individual level for its 2023-2030 Strategy.

Comment on Cyber Security Strategies from 2016-2023

There have been multiple Cyber Security Strategies developed by the Federal Government: in 2016, 2020 and now again in 2023. Each have required significant work by the many organisations who contributed to the public consultation process, as well as input by associated expert boards or panels, such as the 2020 Industry Advisory Panel as it was then known. Acknowledging that cyber security is a fast-moving domain, it is important that the focus be on where threat domains have significantly evolved, where gaps lie, and where

[3] https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf
[4] https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme
[5] https://www.cyber.gov.au/report-and-recover/report
[6] https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure
[7] https://www.asx.com.au/documents/rules/Chapter03.pdf

there can be useful practical measures not already afoot, building on the merits of previous Strategies. A genuinely principles-based Strategy will by nature be extensible and flexible up to 2030.

The AIIA believes that policy coordination on cyber security must be a priority for the government. The AIIA notes that the role of an appointed Cyber Security Coordinator was announced in late February 2023.[8] However, the Discussion Paper released at the same time does not delineate or refer to the role and further information about the nature of the role was left to remarks by Secretary Mike Pezzullo at the Cyber and Infrastructure Security Conference on 24 March 2023. The AIIA would posit that such a significant, whole-of-government role not being raised or enquired about in the industry consultation in response to the Strategy Discussion Paper is not best practice. Further, comments in the media or on social media suggesting that certain conclusions are foregone – such as making the payment of a ransom illegal or that mandatory step-in powers may be extended to 'whole of economy' does not give confidence in the open development of the Strategy.

It is important that the Strategy fully leverages the work industry has put into responding to the *Strengthening Australia's Cyber Security Regulations and Incentives* Discussion Paper[9] and the *National Data Security Action Plan* Discussion Paper.[10] Industry has been informed that these consultations will all be coalesced into the final Cyber Security Strategy 2023-30.

Australia's International Cyber and Critical Technology Engagement Strategy 2021[11], JPC3[12] and the 2022 National Plan to Fight Cybercrime[13] are all bodies and initiatives that do or have existed relatively recently with relevant findings on cyber security and cybercrime strategy. The progress made and directions taken by these bodies should be considered in developing this 2023-30 Strategy.

The AIIA will now address the majority of the questions included in the Discussion Paper.

Q.1 What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Small and Medium Enterprise Capability Uplift

The 2030 Strategy should have an emphasis on Small and Medium Enterprise (SME) Cyber capability, resilience and uplift as a priority, given SMEs account for between 97.4% and 98.4% of all businesses.[14] SMEs collect significant amounts of customer data; represent the majority of trusted advisers such as lawyers, doctors and accountants. SMEs are also set to be included in the purview of the *Privacy Act 1988* if the *Privacy Act* Review Final Report's

[8] https://theconversation.com/albanese-government-to-appoint-coordinator-for-cyber-security-amid-increasing-threat-to-systems-and-data-200699
[9] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives
[10] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security
[11] https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf
[12] https://www.afp.gov.au/what-we-do/joint-policing-cybercrime-coordination-centre-jpc3
[13] https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf
[14] https://www.asbfeo.gov.au/sites/default/files/2021-11/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2_0.pdf

recommendation to ultimately remove the SME exemption is accepted by government.[15] The AIIA supports the inclusion of SMEs under the Privacy Act but notes that some SMEs may require additional cyber support to ensure that they can comply with the legislation.

However, legislation should not be the only tool used to encourage SME cyber security adoption. Funding or financial support by the government to seed SMEs (especially small businesses) towards kickstarting or overcoming the inertia of uplifting their cyber security status would have strong impact. Industry-led and maintained certification for SMEs is another ripe area for development and backing by government. In the UK, the AIIA notes that self-attestation or external assessment through the industry-led, government-backed Cyber Essentials and Cyber Essentials Plus schemes forms the model for certification for businesses regardless of size.[16]

Further, SMEs play an integral role in the supply chains of critical infrastructure entities, as well as defence industry, state, territory and Federal governments. For these reasons they are attractive targets for a range of cyber adversaries to collect sensitive data or, a "soft" entry point for adversaries targeting more sophisticated organisations within that supply chain.

From the outset, it is important that the language and narrative government uses about cyber security is matter-of-fact. Militaristic language of '*attacks'* can be daunting and less relevant for small and medium businesses than considering '*breaches'* or analogously data '*thefts'* (naturally, a concept familiar to many brick-and-mortar small businesspeople).

Reshaping this language and narrative for SMEs is essential in encouraging adoption. For instance, the importance of SMEs for supply chains can be leveraged to demonstrate that an SME's future competitiveness and earnings may be dependent on their own cyber security maturity.

Small Business Cyber Security Assessment Tools

The UK National Cyber Security Centre under its Cyber Aware program has a Free Cyber Action Plan tool which provides personalised plans for small and medium organisations or sole traders to improve their cyber security https://www.ncsc.gov.uk/cyberaware/actionplan. The Plan features mostly binary questions with large, readable print and takes approximately 3 minutes to complete. The Cyber Security Assessment Tool on the business.gov.au website developed by the Department of Industry, Science and Resources is the closest equivalent in Australia, however this is not under the purview of the Australian Cyber Security Centre and general public awareness of the Assessment Tool is low. Language barriers and time-poverty mean that the 20 minutes it takes to complete the tool and interpret the multi-pronged options in each question may be prohibitive.

Cyber Security Concierge Service and Cyber Clinics

The AIIA supports the concept of a Cyber Security Concierge Service for SMEs.[17] While the cyber.gov.au website contains a useful Small Business Security Guide, real-life clinics and a dedicated Cyber Security Concierge Service (which could also take proactive steps to make contact with SMEs) could be more impactful and ensure that resources such as the Essential Eight are made real, bite-sized and relevant for the needs of individual companies.

[15] https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[16] https://www.ncsc.gov.uk/cyberessentials/overview

[17] https://aiia.com.au/wp-content/uploads/2023/04/AIIA-Pre-Budget-Statement-2023.pdf

The 1300 CYBER1 hotline has an Individual and SME Option in the Menu, which takes the caller through to a representative of the ACSC. However, a dedicated Cyber Security Concierge Service would exist for businesses, not individuals, whereby the operator is trained to operate with a sense of service to businesses (rather than individual citizens), run real-time assessments and make practical suggestions, including connecting businesses to high-quality services, products, consultants, trainers and cyber ranges. Real-time equivalents in the form of clinics could run in shopping strips, shopping centres, legal precincts, medical precincts amongst others and could take the form of a mobile Cyber Security check-up service connecting business-specific representatives of the ACSC with SMEs. As a model, government could look to the free 45-minute cyber consultations known as 'Cyber Clinics' provided jointly by the Australian Cyber Collaboration Centre, AustCyber SA Node, and the Government of South Australia's Department for Industry, Innovation and Science.[18]

Cloud adoption, password management, backups, and principles such as data minimisation, least privilege and zero trust could be covered in practical ways. Legal practices, medical practices and accountancy firms are examples of businesses holding sensitive and personal information but that may not have sufficient budgets for internally funded cyber security training sessions or audits. It is noted that the Small Business Guide encourages businesses to regularly train their staff in cyber security without referring to any external providers. Government must build tangible connections between interested or in-need businesses and training that is practical, accessible and where possible, funded or subsidised by government as part of a strategic effort to uplift SME cyber security capability.

The importance of cloud adoption for SMEs

Government must work to accelerate secure cloud adoption throughout the economy, including at the SME layer. With greater cloud adoption, consumers, the community and industry all stand to benefit as a means of uplifting cyber security nationally. The more businesses and data-collecting entities are engaged on services equipped with security teams deploying best-practice cyber security hygiene, training and practices, the better for Australia. Cloud awareness and Cloud fundamentals training must be provided as part of cyber security training and awareness materials. Cloud has particular utility and economies of scale for small businesses, with security systems and teams responsible for cloud-hosted data from much larger organisations with more significant cyber security capability. It is of course important to remember that security in the cloud is a shared responsibility, with Cloud Service Providers (CSPs) responsible for securing their infrastructure and systems and the customer responsible for securing their data stored in the cloud (i.e. restricting access to data on a needs basis).

An existing initiative (not yet law) that could be leveraged is the Small Business Technology Investment Boost whereby, subject to law, small businesses will be able to deduct an additional 20 per cent of expenditure incurred for the purposes of business digital operations or digitising operations on business expenses and depreciating assets such as portable payment devices, cyber security systems or subscriptions to cloud based services.

However, the innocent human element is often at the heart of cyber security incidents.

[18] https://www.cybercollaboration.org.au/cyberclinics

Training in essential behaviours and preventing inadvisable practices – such as sharing credentials with others or revealing sensitive financial information via unsecure messaging platforms – will mean even the most sophisticated of security systems can be obviated. Most data breaches are a result of people and culture considerations, which is the biggest area of improvement for shifting the cyber security dial. Therefore, government must combine awareness and training on essential behaviours, including through public awareness campaigns, with greater cloud adoption.

Launch a large-scale, national cyber security awareness campaign.

Australia has a history of large-scale, national campaigns to educate citizens of all ages about steps to take to reduce certain risks. Well-known campaigns include the "Click-Clack, Front and Back" campaign to reduce the death toll on roads, and the "Slip, Slop, Slap" campaign to promote UV protection and prevent skin cancer. These large-scale campaigns are undertaken at a societal level because there is a common risk to everyone. Cyber security, being a key priority in the national agenda, should be given the same attention. The Australian Government should work with the private sector to develop and launch a nationwide campaign to help Australians understand cyber security and cybercrime and the basic steps they should take to protect themselves. This campaign should address both the threat and provide simple measures that citizens can take to enhance their cyber security (this could be a simple message along the lines of "patch it up, back it up, lock it up"). This campaign should be across all mediums – radio, TV and online.

Advancing Digital Identity and Furthering Data Minimisation

The high-profile data breaches of 2022 wherein personal documents such as drivers' licenses and passports were compromised adds urgency to the task of advancing the Federal Digital Identity System. It is pleasing that the Digital Data Ministerial Meeting on 24 February had in its communique:

> *Ministers endorsed in-principle the draft National Strategy for Identity Resilience, which sets out principles and government initiatives to make Australian identities hard to steal and, if compromised, easy to restore. This is an example of strong intergovernmental cooperation on making Australia safe from threats such as cyber security breaches.*
>
> *Ministers will consider a final National Strategy for Identity Resilience later this year.*
>
> *The Strategy complements development of a Cyber Security Strategy, which the Minister for Home Affairs and the Minister for Cyber Security announced in December 2022.*

In many cases industry retains information in order to comply with legislative requirements, such as in the case of telecommunications regimes. The right balance must be struck, with government considering national security, law enforcement, privacy and the regulatory burden on industry.

There ought to be a minimalist approach to the cases in which collection of information is mandated or performed by default. The collection of information as a proxy for the verification of information is particularly undesirable; government ought to investigate ways to leverage digital identity reforms and the myGov platform to give businesses and agencies confidence about identity verification via proxy (with reference to a trusted senior government agency) without requiring a from-first-principles approach to ID.

Secure digital identity frameworks, and particularly the model adopted by the NSW Government, shows the merits of such a regime where, once identity is verified, source documents are not kept or required. Government needs to support a mindset shift by providers of services and collectors of information to move away from the attitude of collecting personal details by default. Progressing digital identity and thinking expansively about the role of the myGov platform will be key to allowing this shift to take place.

Cyber Security Strategy work undertaken at the State level

On the matter of States and Territories, the Federal Government must ensure that States who are developing their own Cyber Security Strategies deconflict their work and initiatives with federal activity, noting that while State and Territory Governments must ensure the cyber security of their systems and agencies, leading on cyber security policy and strategy is primarily a federal responsibility. Federalising cyber security from a policy and strategy perspective with national standards for legislation, strategy, policy and policing to which States may align their activities, would help streamline and focus investment and resources. It is particularly important that citizens within respective States and Territories understand that cyber security reporting occurs at the federal level.

Cyber security for the health sector

Cyber security considerations for health systems and health data are of paramount importance. There is a concerning and increasing number of attacks on health data due to the sensitivity and value on the black market of such data.

To engender take up of digital health technology by consumers, clinicians and patients, they must be assured of the privacy and security of virtual care-enabling platforms. Patient information, videos and still images must be stored securely and the nature and location of their secure storage must be effectively communicated to users. Video interface platforms must be dependable and secure. Health data is valuable when it falls into the wrong hands, including on the dark web, where the black market value of a health record (up to $1000AUD) exceeds that of even financial data. The health sector has increasingly been targeted by cyberattacks such as ransomware attacks, with patient data stolen and healthcare delivery services crippled. Health is in the top three industries affected by security breaches. There is an inherent vulnerability in connectivity, and the security implications of sensitive patient-clinician data interactions must be considered. Clinician and patient endpoints are the most challenging to secure, particularly if they are in the control of the patient and the patients' systems, which will vary, or if there is a hybrid of email and video communications taking place. With patients becoming a participant in the security process themselves, there has been opened up a new frontier in the securitisation of clinical systems, requiring deeper community engagement about cyber-awareness and safety.

There must be a greater allocation of funding and resources for IT security for all agencies, hospitals and practices. We must move from the initial reaction to longer-term solutions, to create reliable, available, relevant, complete, secure platforms.

Fast Healthcare Interoperability Resource (FHIR)

In particular, more work is needed on standards, interoperability and industry adoption of FHIR (Fast Healthcare Interoperability Resource) as created by the Healthcare Level Seven International (HL 7). This is the modern, web suite of API technology that is recognised by the USA's JASON taskforce as the current best candidate for health information exchange and access.

The AIIA is calling for the development of a national roadmap for greater industry adoption of FHIR. This would include the development of pilot projects and use cases, noting that in the US, government spearheaded the Argonaut Project along with members of the private sector to advance industry adoption of modern, open interoperability standards such as HL7 FHIR

The Government must work towards a national agreement with general practice organisations and clinical systems vendors to move to cloud-based software by end 2024 in general practice and primary care to advance cyber security capability and protection levels across these significant components of the health care sector.

Q2. What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

The Discussion Paper states:

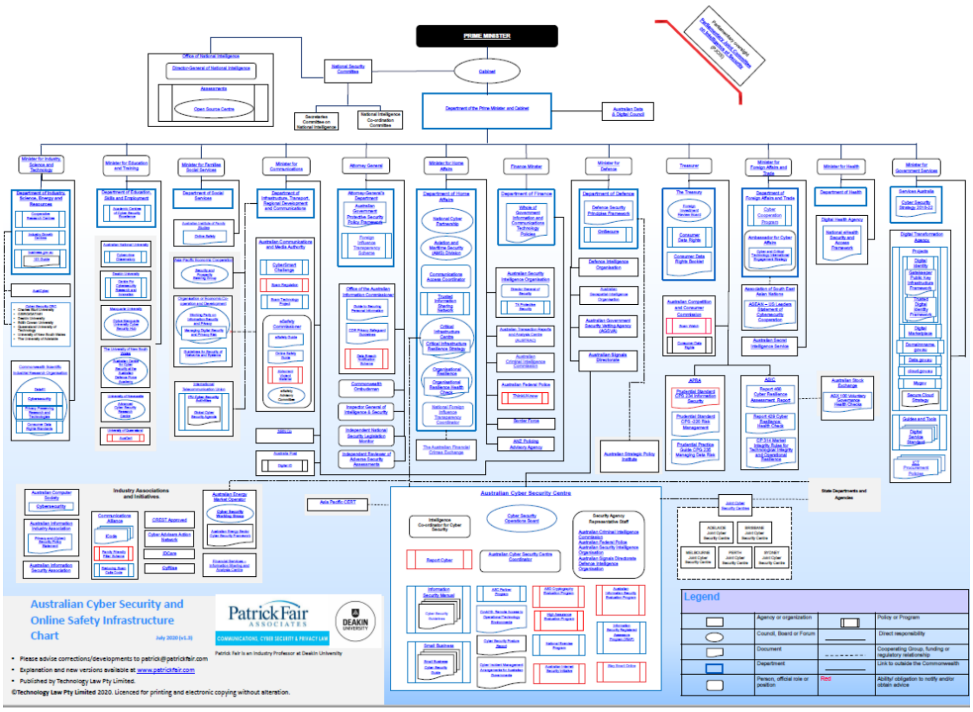
"It became clear during these incidents that government was ill-equipped to respond, and did not have the appropriate frameworks and powers to enable an effective national response given the number of Australians whose personal information, including identity data, was compromised."

The 2022 Optus and Medibank cyber hacks to which the Discussion Paper ostensibly refers have highlighted the nature of scale of personal data that can be compromised, with governments and citizens rightly asking why so much personal data needs to be stored. Government needs to provide clarity and guidance on this matter so private sector companies can clearly understand their legal obligation around retention. The role and responsibility of boards and treating data as a liability as well as an asset is a relatively new development.

This clarity, guidance and assurance from government is where the opportunities for greater resiliency and data security lie.

Further, the complicated nature of cyber policy and regulation creates not only cost on the economy but also confusion as to the regulations themselves. Lawyer and technologist Patrick Fair has summarised the cyber security legislative and regulatory landscape in the following infographic:[19]

[19] https://www.patrickfair.com/_files/ugd/ce391e_546b5b105fe64af79037d0d2fe70d329.pdf


PRIME MINISTER
Cabinet
Department of the Prime Minister and Cabinet
Industry Associations and Initiatives
Australian Computer Society
Cybersecurity
Australian Information Industry Association
Australian Information Security Association
Communications Alliance
iCode
CREST Approved
Cyber Advisers Action Network
IDCare
CyRise
Australian Energy Market Operator
Asia Pacific CERT
Australian Cyber Security Centre
Legend
Australian Cyber Security and Online Safety Infrastructure Chart
July 2020 (v1.3)
Patrick Fair Associates
COMMUNICATIONS, CYBER SECURITY & PRIVACY LAW
DEAKIN UNIVERSITY
Patrick Fair is an Industry Professor at Deakin University
Please advise corrections/developments to patrick@patrickfair.com
Explanation and new versions available at www.patrickfair.com
Published by Technology Law Pty Limited.
©Technology Law Pty Limited 2020. Licenced for printing and electronic copying without alteration.

Any organisational, regulatory or legislative interventions by government must be measured against the extent to which they simplify the current landscape of reporting and responsibility for cyber security within the Federal Government.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Certain initiatives under the Critical Infrastructure legislation such as the Risk Management Program (RMP) have only just gone live for industry with reporting requirements starting in 2024. Notably the telecommunications sector is still working through the interaction between the SoCI regime requirements and the Telecommunications Sector Security Reforms (TSSR), a complex undertaking. The AIIA's members are reluctant to see the legislative and regulatory goalposts shift yet again before there is the opportunity to comply with new regimes, consider the proposed changes in the existing privacy regime, and evaluate the business impacts of such existing artefacts of law and regulation. Where legislative interventions are fresh they should be allowed to make their impact and be absorbed by industry in terms of compliance and evaluation. No further categories within Critical Infrastructure are required and considering 'customer data' and 'systems' as 'critical assets' would present myriad issues and questions for industry and government alike. Expanding the SoCI regime to customer data and 'systems' would not meet the original definitions pertaining to social and economic stability, defence and national security under which assets were at the outset deemed to be 'critical'; and importantly, if an expansive set of assets is deemed to be 'critical' the very conception of 'critical' asset will be rendered less meaningful. Instead, government focus should shift to advancing the digital identity system to address systemic issues and opportunities around easing unnecessary collection of personal data.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

It is not necessary to add specific obligations for cyber security to Directors' Duties. Directors are already required to consider cyber security related issues within the duty to act with reasonable care and diligence (Section 180 of the *Corporations Act 2001*). Each category of directors' duties does not need to be addressed by specific legislation.

As it stands, a significant incident can occur on the basis of an area of a company no Board member would have significant oversight over, so imbuing a Board Director with liability for cyber security risks and consequences in an explicit or granular sense is not conceptually sound. The practical question is instead how board directors can reasonably satisfy themselves that they have met existing obligations, and how organisations can bring cyber security officers within organisations into direct contact with board governance.

It is of critical importance that Chief Information Security Officers (**CISOs**) have a 'voice to the Board' and are in a position to articulate cybersecurity and IT operations into the risk profile of entities that is effectively communicated to boards of directors.

The Telstra Five Knows of Cybersecurity[20] – Know the value of your data; Know who has access to your data; Know where your data is; Know who is protecting your data; Know how well your data is protected – may be useful in helping Board members understand what they need to start asking questions about, which is the first step in effective risk management practices. Clear guidance and frameworks in place pertaining to core areas of risk and sensitivity, helping board members navigate complexity and granularity with realistic expectations. Modern Slavery legislation and WHS requirements are analogical externalised requirements on Boards with which Directors in Australia have gotten to grips.

A sound analogy is that Board members need not to be able to analyse an entire statement of accounts, but they should be able to read and understand end-of-year financial statements as a barometer for their financial soundness.

The APRA Prudential Practice Guide[21] is a sound model for Board directors, which includes security principles and awareness of all users, including contractors. Cyber security principles called out by the Guide which are useful for Board Directors include:

- Defence in depth
- Least privilege
- Never trust, always identify
- Assumed breach

Government should consider implementing basic cyber security training and familiarisation based on sector as a training intervention tied into the process of individuals becoming Board Directors in concert with the Australian Securities and Investments Commission (**ASIC**). The AIIA notes the important work of the Australian Institute of Company Directors (AICD) in developing the Cyber Security Governance Principles in cooperation with the Cyber Security Cooperative Research Centre, including a checklist for SME and NFP directors.[22]

[20] https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf

[21] https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf

[22] https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html

The AIIA also notes that while there are obligations and responsibilities for boards across the private sector, there are not necessarily the same obligations and responsibilities levelled on Heads of Government Departments and Agencies nor responsible Portf olio Ministers. The Government should explore this as part of the strategies development.

d. Should Australia consider a Cyber Security Act, and what should this include?

The AIIA considers that given the existing Privacy Act and Critical Infrastructure legislation (CI SoNs), a new Cyber Security Act is not required. By nature, in Australia, cyber security is a feature of cross-cutting legislation pertaining to data, technology, critical infrastructure and personal information. However, if the Government is to codify cyber security obligations in legislation it must usefully consolidate and streamline such obligations, not extend them. Anything novel must amalgamate and replace, not be functionally additive or complexifying. The AIIA does support the simplifying and removal of duplicative regulatory requirements leading to a well-understood, principles-based cyber regime which would remove the need for a single act. The Cyber Security Coordinator and better policy and regulatory coordination from government are important reforms the Strategy should address and recommend.

In considering whether to move towards a Cyber Security-specific Act, the Strategy must determine the definition of 'cyber security' for its purposes; articulate which gap it is attempting to fill; the reason for which new legislation is being introduced; and the implications for existing legislative and regulatory frameworks. We would also encourage the Australian Government to look to and align Australian laws with international best practice.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

The AIIA has been advocating for a Council of Tech Regulators that would bring together the agencies and departments within the Federal Government possessing regulatory engagements with implications for data, ICT, Cloud and digital platforms and cyber security. While the AIIA acknowledges that cyber security is inherently complex with multiple regulators and Acts involved, such a body could ensure the sequencing and streamlining of reporting requirements, regulation and industry consultation processes to ease burdens on industry.

Government should monitor regulatory burden on businesses in respect of legal cyber security obligations by seeking voluntary cost estimates from affected businesses. While the cost impacts of discrete legislative regimes such as SoCI have been sought in cases, the additive nature of the cost burden inherent in cascading and multiple regimes should be considered by government. One of the mandates of a Council of Tech Regu lators could be a holistic cost impact study of tech regulation.

Furthermore, the sheer complexity and number of regulating agencies and bodies within government is a measure of regulatory burden. The multiplicity and time-variance of reporting requirements, plethora of information requests and engagements from multiple government agencies with entities affected by a breach is another measure of regulatory burden. This has be recognised by government when it announced its Office of Cyber

Security Coordinator. As mentioned earlier in this submission, better coordination of policy and regulatory frameworks by government should be an immediate priority.

f. *Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:*

(a) victims of cybercrime; and/or
(b) insurers? If so, under what circumstances?

The AIIA understands the government seeking to make entities less desirable targets to cyber criminals. However, the government should not explicitly prohibit the payment of ransoms and extortion demands, as it would just penalise victims further and discourage reporting of ransomware and related attacks. Instead, government should focus on articulating best-practice in response to a ransomware attack. Under "instrument of crime" provisions in Division 400 of the Criminal Code Act 1995 (Cth) and AUSTRAC legislation, there are arguably already stipulations in place regarding payments of ransoms. Ransomware incidents should be viewed within a risk context. There need to be clear alternatives and mechanisms for recovery articulated by government guidance for entities affected. Converting the victim in a ransomware attack into the criminal in circumstances in which the instigator of the ransomware attack will almost always not face consequences would appear a perverse outcome, especially where the victim is a small business.

The International Counter Ransomware Task Force (ICRTF) under the Counter Ransomware Initiative that Australia chairs, with its focus on cross-sectoral tools, cyber threat intelligence exchanges and collective best practice guidance for countering ransomware, has the appropriate focus for combating ransomware both locally and globally.[23]

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Clarification is desirable and the rationale for not paying ransoms is understandable, but this should not be made a crime as it would further penalise victims of these attacks.

Q3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Australia should provide intelligence threat-sharing cyber hubs in the region, such as the Cyber Threat Alliance (**CTA**) which is discussed further below in the answer to Question 7. Australia should also ensure that cyber security and technology policy experts are situated at international posts under the Department of Foreign Affairs and Trade and in cooperation with the existing position of Ambassador for Cyber Affairs and Critical Technology to contribute to the international conversation, efforts and threat-sharing regarding cyber security across our international diplomatic apparatus.

Q.4 What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

The AUKUS Opportunity

[23] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/counter-ransomware-taskforce

Government has a role to play in supporting the technology sector to realise the opportunity of the important trilateral AUKUS alliance. Government should seek alignment, interoperability and opportunities for cyber security uplift as Australia seeks to avail itself of the AUKUS opportunity in areas beyond defence, as well as examining the cyber security and technological aspects of the agreement's key performance indicators, including alignment of standards and certifications, industry's role in deploying technology at the cutting edge of innovation for strategic interests, and achieving interoperability with trusted standards. Deploying this agreement against a complex geostrategic backdrop in the 21st century will also require aligning international partnerships underway in the critical technology space, including in quantum research and development. Other alliances, including the QUAD, should be leveraged with a cyber security component and a focus on interoperability and mutual recognition. As per the proposed Quantum Strategy, international partnerships in research and commercialisation will be essential for Australia's critical technology future so it is important that alliances are leveraged for cyber security outcomes and alignment along parallel lines.

AIIA Pacific Digital Capability Uplift Program

The AIIA, in February 2023, delivered an impactful program in the Pacific leveraging the global skills and capability from Australia tying into the Australian Government's strategic engagement with the Pacific, which forms a worthy basis for future engagement in cyber security uplift in this region.

As leading global economies such as Australia are becoming increasingly digitised, the AIIA believes that they must play their part to ensure Pacific Island nations are not left behind on this digital maturation journey. As such, the AIIA delivered a collaborative digital capability uplift program in Suva, Fiji, aligning to Australian government strategic interests, providing support for near Pacific Island neighbours and supporting Australian industry.

Representatives of the local Fijian government, chambers of commerce and Pacific Islands Forum gave their support on panels, as attendees and in organising as well as support from Austrade and the Australian High Commission. The program intentionally mixed traditional training from technical experts and presentations by tech thought leaders with interactive panels filled with locals with opportunity for live feedback. As a pilot, the program was successful in execution, leading to genuine partnerships built with ongoing engagement between Fiji and the Australian tech industry and wider Pacific.

The AIIA conducted a post-event survey with extremely positive responses, which is instructive to guide future outreach. 75% of respondents rated the program “very” or “extremely” valuable, 90% of respondents rated the organisation of the program “high” or “very high” in quality with Cybersecurity the most valued topic at 70% of respondents.

Local Stakeholders included the Fijian Ministry for Communications, the Fijian Ministry for SMEs, Trade and Co-operatives, Fiji's Trade Commissioner (Sydney Consulate), Austrade / Australian High Commission, Outsource Fiji and the Pacific Islands Forum Secretariat. This model should be leveraged and funded into the future for cyber security uplift amongst Australia's Pacific neighbours.

Q.5 How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Australia, which has a proud history of standards development domestically, should be engaged globally in the development of standards. This would ensure the dual outcome of both Australian companies being able to export goods and services with confidence knowing that standards are consistent across economies but also would mean Australian cyber security requirements are advocated for in these global standards development contexts. Where possible and practical, Australia should leverage international standards.

The AIIA notes the Cyber Taskforce to Drive Standards by the Australian Government together with the Cyber Security Best Practice Regulation Taskforce included the following actions, and work attendant to each of these three Actions should be assessed and built upon:

- Action 1.2A – Support Australian participation in the development of international standards
- Action 1.2F – Government and industry will jointly use Industry Growth Centres to promote best-practice Australian and international standards through the Growth Centres' international networks
- Action 1.2G – Work with Standards Australia to identify Australia's interests in the development of international standards.[24]

Q.6 How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Hardening government systems; risk-based decision-making around supply chain risks

Government must 'get its own house in order' and as a priority harden government systems and IT, mirroring the onus that is placed on the private sector in respect of cyber security. The AIIA notes that in the United States, a recent executive order required government agencies to only purchase software that meets secure development standards, so as to protect government data. To support such an order, in February the National Institute of Standards and Technology (**NIST**) issued guidance that provides federal agencies with best practices for enhancing the security of the software supply chain. Two guidelines were released: the Secure Software Development Framework and the Companion Software Supply Chain Security Guidance.

Further, cyber security and supply chain security should be a consideration for government in its consumption of ICT services, alongside criteria such as 'value for money'. A holistic gap analysis should be undertaken prior to changes to Procurement Rules to ensure that they are not duplicating with existing ICT assurance and compliance apparatus and do not replicate existing frameworks.

[24] https://www.services-exports.gov.au/progress/cyber-taskforce-drive-standards

Establishing greater awareness of supply chain issues to enable risk-based decision-making by procuring governments should be considered. This will require a mature and longer-term conversation between industry, the federal government, and allied governments that have approached similar issues.

New Government Policies Needed on Key Security Principles – including Zero Trust and Attack Surface Management.

The AIIA would encourage the Federal Government to develop advice on the below two key security principles that are core to improving and hardening Government and critical infrastructure. These two pillars have already been identified by the US Government as core security tenants with agencies asked to implement these principles in their own environment.

- **Guidance and mandates requiring agencies to adopt zero trust architecture.** Zero Trust is a strategic approach to cybersecurity that secures an organisation by eliminating implicit trust and continuously validating every stage of digital interaction. Zero trust is not a product, but a security framework. It is a way for government agencies and departments to build resilience into their IT environments. The Zero Trust Model has become increasingly important for the US federal government due to President Biden's unprecedented Executive Order on Improving the Nation's Cybersecurity and the more recent federal Zero Trust architecture strategy from the U.S. Office of Management and Budget (OMB).

- **Guidance and mandates requiring Government agencies and critical infrastructure to have attack surface management capabilities.** In today's world, it is critically important that organisations understand what their network looks like through the eyes of an adversary. Today, attackers regularly scan the internet to find vulnerabilities in public facing infrastructure and exploit them. Attack surface management is the process of continuously identifying, monitoring and managing all internet-connected assets, both internal and external, for potential attack vectors, exposures and risks. Attack Surface Management principles are founded in the understanding that one cannot secure what one does not know about. Mandates that Government Agencies must have visibility over their network attack surface in several key Government documents and policies in the US and EU.[25]

- **Review Roles, Responsibilities and Investment Across Government Agencies** – government must examine the level of security (not merely ICT expenditure) expenditure across government agencies and ensure that all government agencies have a Chief Information Security Officer or similar role and that they are accountable to the Secretary in their own right.

Q.7. What can Government do to improve information sharing with industry on cyber threats?

Engagement with the Cyber Threat Alliance

[25] National Defense Authorization Act (NDAA), Federal Information Security Management Act (FISMA) Reform Efforts; EU Network and Information Security Directive (NIS2)

The Cyber Threat Alliance (CTA) is a not-for-profit organisation that works to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organisations in the cybersecurity field. It is the cybersecurity community's first automated cyber threat information sharing organisation, now comprised of over 30 of the world's leading cybersecurity providers. The CTA works with key industries information sharing organisations: DIB-ISAC, FS-ISAC, ICS-ISAC and Other threat intel communities. Since inception, the CTA has regularly exchanged information on botnets, mobile threats and indicators of compromise (IoCs) related to advanced persistent threats (APTs), and advanced malware samples.

Undertake Targeted and Tiered Engagement with the Private Sector.

Government should build out a multi-tiered engagement model for public-private partnerships. Consideration should be given to multi-tiered engagement structures that group government and industry partners together in ways that best align to mission objectives and the nature of the desired relationship. We recommend that groupings be established around public and private sectors, and around the desired communication flows (i.e. unidirectional versus bidirectional).

To expand, while some organisations may be consumers of Australian Government cyber security threat intelligence (i.e. some CI sectors and small-medium businesses), others (i.e. sophisticated technology or cyber security organisations) may be able to meaningfully contribute to the Australian Government's threat intelligence and support disruption efforts. The information and messaging around particular threats and vulnerabilities pushed out to these organisations should also be adapted to recipients' level of cyber security capacity.

Q. 8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

The AIIA indeed believes that an explicit obligation of confidentiality upon the ACSC would assure entities are encouraged to give full disclosure with a focus on the containment of the cyber breach. Furthermore, as the AIIA suggested in its submission to the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* inquiry, if the government does pursue the path of setting out examples or gold standards of steps, there should be a safe harbour relief from penalties for organisations who have engaged in timely reporting, acted in good faith and worked to sound data and cyber security practices with due diligence.

Q.10 What best practice models are available for automated threat-blocking at scale?

Security Operations Centres automation

Today, cyber-attacks as well as cyber security defences leverage machine learning and automation. If organisations try manual defence against automated attacks, the fight becomes human-versus-machine, with highly unfavourable odds for the human-driven organisation. Successfully protecting against automated attacks necessitates incorporating automation into cyber defences- including security operations centres (SOCs). This levels the playing field, reduces the volume of threats, and allows for faster prevention of new and previously unknown threats. Automation also supports real-time incident response at scale to triage and respond to attacks faster. Automating SOC functions can also significantly benefit staffing – low-level threats are addressed by automation, freeing up highly-skilled (and finite) staff resources to address more sophisticated attacks.

Threat-blocking at scale

There are numerous examples of global efforts to block cyber threats using predictive methods. Notably Telstra employs automated threat blocking with upscaled Domain Name System (DNS) filtering, where millions of malware communications are automatically blocked each week. Another example is quad9, a global threat filtered DNS service that is publicly available. Vendors engaged with quad9 apply advanced analytics (i.e. AI) to not just block known threats, but predict domains that are part of an attackers campaign to cause damage. This same, interconnected, global model has several other examples in the corporate community. The key is that Australia needs to ensure that global connectivity and scale is also used to increase accuracy of threat blocking to reduce false positives to close to zero.[26] Finally an AIIA member has partnered with an EU government to deploy firewalls across its entire national-level ISP infrastructure to protect its government, citizens, and businesses at scale from cyber-attacks launched by various sophisticated state-based actors.

DNS filtering could be complemented by additional steps and technologies to automatically block threats at scale before they execute into cyber attacks. As such, the Government could consider as best practice prioritised enterprise-grade cyber security considerations (including the Zero Trust security principle; consistent and granular visibility of threats; and an automated approach to security enforcement) and investments in SP/ISP network planning and buildouts, particularly as Australia moves to 5G. Government could collaborate with industry partners to consider the feasibility and adoption of at-scale approaches, such as how SPs and ISPs can effectively be incentivised towards adoption.

The AIIA would note that the capacity and resources to block threats varies widely between different telecommunications organisations and ISPs. A national feasibility study seeking a lay of the land as to current threat-blocking activity, definitional clarity around threat-blocking, an examination of the different kinds of architecture and the points at which threats may feasibly be blocked for organisations of various size and resources would be desirable.

Q. 11 Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Growing cyber security talent is a vital and welcome focus. The skills shortages and experience gaps affecting the cyber security industry mean government and industry need to widen and strengthen the skills pipeline as well as retrain and employ more cyber professionals to meet business and community need. The Government should consider attracting talent through financial incentives such as government-funded scholarships that

[26] https://www.quad9.net/service/threat-blocking/

will attract and incentivise people into the industry. Any financial incentive should include a return-to-service obligation, ensuring graduates undertake a number of years in key government agencies at the completion of their funded studies.

The Government should clearly define which skills Australia needs, and why, noting the role of automation, the ageing population, and the significant personnel supply issues faced by the industry, this may mean that roles need to evolve and automate in the future for the cyber security workforce to sustainably meet societal goals. For example, many low-level tasks within a Security Operations Centre (SOC) can – and should – be automated or responsibly augmented by Artificial Intelligence. This should be a consideration in performing a skills need audit. Government also ought to leverage existing industry activities, such as SkillFinder.[27] The Government should also work with hiring managers and industry leaders to reset qualification expectations and shift mindset about the necessity of a Bachelor's degree.

Finally and crucially, government must work to bridge the gender gap in cyber security whereby women constitute just 17% of the profession,[28] including by emphasising the importance of both hard and soft skills, the sheer breadth of the cyber security industry, breaking down misconceptions about a narrow required background or skillset and promote case studies of career changers and women with non-STEM backgrounds in cyber security.

Q. 12 What more can the Australian Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

It is important that work on the professionalisation of the Cyber Security industry align to respected international frameworks and standards and focus on encouraging people of all backgrounds into the industry, while advancing trust, confidence and clarity amongst the cyber security ecosystem in a meaningfully industry-led manner. The AIIA sits on the Australian Cyber Security Professionalisation Program's co-design group.

Q. 16 What opportunities are available for Government to enhance Australia's domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

If government can make domestic capability a priority for the cyber security industry, a greater proportion of the Retained Economic Benefit (REB) pertaining to cyber security products and services will be secured domestically. Cyber security market growth, greater market opportunities for Australian cyber security businesses and the capacity to establish export capability in cyber security as an area of strategic significance is another opportunity available for government as a partner in building the domestic cyber security industry. However, the AIIA would emphasise that the engagement and procurement activities between Australian government departments at all levels and Australian cyber security companies has been limited and industry development is currently immature.

Greater traction, work and contracts in the cyber security space from government will be required for the Australian cyber security industry to gain traction. Despite an increase in the sheer number of cyber security companies in Australia as reported as 350 domestic entities by AustCyber in 2020, 88% of that number have fewer than 100 employees and SMEs

[27] https://www.skillfinder.com.au/
[28] https://ia.acs.org.au/article/2023/just-17pc-of-australia-s-cyber-workers-are-women.html

received $800m in revenue, one-quarter of the sector's total revenue in 2020.[29] With the vast majority of these organisations being very small, and competing with other another for similar work, there is a lack of a genuine domestic ecosystem with the attendant opportunities for cohesion, diversification and partnership. Anecdotally the AIIA has heard of Australian cyber security companies experiencing greater traction in overseas export markets than in the domestic government procurement market. Government must prioritise a nucleus of domestic capability in-country before export becomes a focus for Australian cyber security products and services. The aim to harden government infrastructure must be seen as an opportunity to both procure from and thus build capability in Australian cyber security companies and consultancies. Certainty and a strategic agenda for cyber security industry development from government would allow the domestic sector to coalesce, focus and plan around government demand.

From a sectoral perspective, the AIIA is eager that Project REDSPICE, an encouraging and visionary initiative, incorporates domestic capability as an objective of this Strategy in the practical way that recruitment and personnel for the Project is managed, whereby Project REDSPICE meaningfully partners with organisations to move the needle on domestic capability, grow the cyber security talent pool and see personnel retained within domestic industry long-term.

Finally, the Government should leverage the three points of AustCyber's Sector Competitiveness Plan:

1. ***Support research, innovation and startup development –** Increasing R&D funding through ARC grants and increasing the scope and clarity of R&D tax incentives will support cyber security research and industry development. Continuing to collaborate across sector stakeholders and mature the innovation hubs will support a stronger innovation ecosystem.*

2. ***Bolster domestic procurement and export capability –** Ensuring that government procurement processes are accessible to small, local firms will support continued growth in domestic revenue. Continued trade outreach, including trade delegations, export support and study tours, will facilitate export growth.*

3. ***Attract local and international talent –** Providing incentives and support for school leavers and skilled workers to train in cyber security will strengthen the cyber talent pipeline. Increasing the number of cyber security skilled migrants will mitigate short-term shortages.*[30]

Q. 17 How should we approach cyber security technologies future-proofing out to 2030?

Quantum cryptography

From a cyber security uplift perspective, quantum computing can protect devices in space that are of a military or other critical nature using advanced quantum key distribution (QKD) cryptography, with quantum realising efficiencies using symmetric keys rather than asymmetric keys, which often rely on space-situated missions for the refinement of the cryptography. QKD saves time and resources by enabling the issuing of new, tamper-

[29] https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1

[30] https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020

evident keys to space assets without pre-coordination, post-field deployment. China is a prime mover in using quantum keys and entanglement-based QKD in space.

Both the applications and challenges presented by quantum technology when it comes to de-encrypting data and cryptography should be front of mind for governments. As recommended in *Growing Globally Competitive Industries*,[31] the AIIA's 2021 White Paper, "government needs to dedicate resources to identify the potential quantum-era security exposures across all departments and keep abreast of the developments in post-quantum cryptography standards, to implement solutions as they become available." Cyber security futurists with an understanding of future quantum applications must be embedded in both research and industry ecosystems, and organisations must be 'quantum-ready'; Canberra-based Quintessence Labs has developed quantum resilience products for global corporate clients in light of HNDL (Harvest Now, Decrypt Later) attacks.

Leveraging automation to detect, prevent and respond to cyber security attacks

Today, both cyberattacks and cybersecurity defences are leveraging machine learning and automation. An automated attack is one performed by a computer program rather than the attacker manually performing the steps in the attack sequence. If organisations try to defend against these attacks manually, the fight becomes man-versus-machine, with highly unfavourable odds for the organisation. To successfully protect against automated attacks, it is essential to incorporate automation into cybersecurity efforts. Automation levels the playing field, reduces the volume of threats, and allows for faster prevention of new and previously unknown threats. Automation also supports real-time incident response.

Security settings must be considered as Australia builds up new technologies and components of the nation's digital backbone. For example, as industry moves towards 6G research and development, security must be implemented into protocols and operations by design.

Q. 18 Are there opportunities for Government to better use procurement as a lever to support the Australian cyber security technologies ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Culture shift to Government as a procurer of technology goods and services.

Cyber and information security was one of the priorities for local investment identified by the AIIA's Domestic Capability Policy in 2021.[32] Cyber-enabled threats and attacks pose threats to both security at the citizen level and the national level. Therefore, providing cyber security has direct links with the concept of domestic capability, which is at its essence the ability for a nation to respond to unforeseen events and provide sustainable, uninterrupted delivery of products and services that enable the operation of critical industries.

Australian Government agencies are still developing "in-house" capabilities even when there are commercial off-the-shelf (COTS) solutions available. COTS solutions have many advantages (particularly in the security space) as they typically have significant capital poured into their Research and Development and leverage global threat pictures to enhance the security services and offerings. COTS solutions can also help with the cyber security

[31] https://aiia.com.au/wp-content/uploads/2021/08/AIIA-Growing-Globally-Competitive-Industries.pdf
[32] https://aiia.com.au/wp-content/uploads/2021/06/AIIA-DC-Framework-Policy-2021-1.pdf

skills challenge - as they can redeploy skilled and cleared staff who are maintaining or building solutions, to other mission critical or priority tasks.

It is important that efforts to better use procurement as a lever be aligned, through engagement with the Department of Finance and the Department of Industry, Science and Resources, to the Future Made in Australia Office and Buy Australian Plan. It will take the Department of Home Affairs, the Office, and the two responsible Departments, working together to effect the structural changes necessary to effectively pull this lever. It may require specialised units to work across government in respect of security and cyber security procurement.

Government purchases should be secure-by-design and procurement decisions are made with cyber security in mind. Procurement should consider both cyber security and supply chain security. The AIIA acknowledges that value for money is an important public sector value, with it being of paramount importance that public money is spent efficiently, effectively, ethically and economically. However, price is not the sole factor in procuring goods and services; government officials ought to consider non-financial benefits associated with a procurement, especially technology-related procurement. The security of the technology in question and the product's integrity with respect to supply chain security ought to be prime considerations. This could be prompted and supported by amending guidelines and supporting policy to encompass the importance of cyber security and supply chain security.

Q. 19 How should the Strategy evolve to address the cyber security of emerging technologies and promote security-by-design in new technologies?

The AIIA notes recently released guidance[33] from the ACSC together with the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) and international partners in Canada, the United Kingdom, Germany, the Netherlands and New Zealand urging manufacturers to '*revamp their design and development programs to permit only Secure-by-Design and Default products to be shipped to customers*'. The recommendations should be considered as part of this Strategy, with a focus on ensuring practical guidance to all industry players including SMEs. The AIIA notes that the resources and toolkits developed by the ACSC for Industry are limited to guidance for IoT manufacturers and would encourage more focus on development of Australian-specific guidelines that coalesce with the Software Product Security Principles outlined in the recommendations. The AIIA would be pleased to act as a conduit to the Australian software industry in this regard.

Further, the Australian Government should work with allied governments to consider how it can develop and promote policies to secure IoT devices. This should leverage the IoT international standards ESTI EN 303 645. If the Government was looking to mandate standards of security in line with ESTI EN 303 645, we would recommend that only the top 3 requirements be mandated. These are identified as the highest priority to achieve the greatest security benefit, while also noting the complexity and cost associated with

[33] https://www.cyber.gov.au/sites/default/files/2023-04/Principles-and-Approaches-for-Security-by-Design-and-Default.pdf

implementing all standards as articulated in ESTI EN 303 645. These are:

1. No universal default passwords.
2. Implement a means to manage reports of vulnerabilities.
3. Keep software updated.

We understand the Government's desire to provide some standardised way for companies to communicate with the consumer regarding the level of security of their IoT device. However, we suggest that there may be merit in exploring some more dynamic ways to do this via digital labelling of IoT devices. This could include providing a link to a webpage where companies can articulate their alignment with the top 3 - 5 standards of ESTI EN 303 645. This would allow companies to dynamically update their alignment with these standards as new information comes to light.

Q. 20 How should Government measure its impact in uplifting national cyber resilience?

In conclusion, the government should not merely look to the number of cyber incident reports received in the year 2030 to discern whether Australia has become the most cyber-secure nation by such a time. Indeed, greater numbers of reports will be made as awareness and detection improve. Instead, levels of community literacy and awareness; adherence to cyber security best-practice by Boards and organisations; essential behaviours becoming second-nature to Australian individuals; and patterns of effective containment and response measures following a breach should be measured to determine whether Australia has seen the uplift in cyber resilience that we need to achieve as a nation.

Thank you for the opportunity to submit a response to this Discussion Paper. Should you have any questions about the content of this submission, please contact

[redacted]

Yours sincerely

[redacted]

Simon Bush
CEO
AIIA