Amstelveen Pty Ltd
ABN: 54 615 045 531
Level 11, 570 George St
Sydney NSW 2000

14 April 2023

Cyber Security Strategy Expert Advisory Board
Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

[Submission via Webform]

Members of the Expert Advisory Board,

Re: Response to Discussion Paper – 2023-2030 Australian Cyber Security Strategy

Amstelveen welcomes the opportunity to provide feedback on the 2023-2030 Australian Cyber Security Strategy.

Amstelveen is a specialist risk and compliance consultancy which operates across Australia and New Zealand. Our clients include private and public sector organisations with a heavy focus on cyber security related risks, such as those in financial services, telecommunications, energy and transit.

In this submission, we have responded to a subset of the questions listed under Attachment A of the discussion paper (titled '2023-2030 Australian Cyber Security Strategy').

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?

We believe that the following three elements would contribute to achievement of the vision of Australia being the most cyber secure nation in the world by 2030:

- **A National Digital ID Service:** To enhance cyber security in Australia, we recommend the implementation of a national digital ID service, similar to those adopted by Nordic countries. With a 98% adoption rate of digital IDs in these nations, there has been a significant reduction in identity-related scams. One of the key contributors to the successful rollout of digital ID across these countries and others was the collaboration between government and banks. Partnering with banks would take advantage of the inherent trust the public has in our banking institutions. A national digital ID service would eliminate the need for sharing physical identity documents with services such as telecommunications providers, banks, credit agencies, real estate agents,

rental companies and similar, which would significantly reduce the risk of identity theft and fraud.

- **Addressing SMS and Call-based Cybercrime:** SMS and telephone calls are the primary ways that criminals monetise data obtained through cyber-attacks. Current solutions, such as Scamwatch administered by the ACCC are inadequate. We suggest implementing a national strategy that incorporates mobile operating system providers, telecommunications providers, and other relevant stakeholders, to address this issue in a more integrated and effective manner, such as with improved information sharing among these parties.
- **A Publicly Available Vulnerability Scanning Service:** A publicly available vulnerability scanning service should be considered, such as the service provided by BitSight. Businesses could register, authenticate, and review any detected vulnerabilities through the external scan. This would provide a valuable resource for organisations to proactively identify and address potential security issues in their digital infrastructure. It could also be used to assign each organisation a cyber risk rating, similar to the operation of credit ratings, that could be used when government agencies and organisations perform customer or supplier due diligence which would help improve supply chain security.

2b. 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?

Given the recent reforms to the *Security of Critical Infrastructure Act* (SOCI), and timeframes to enable critical infrastructure providers with the opportunity to meet these compliance requirements, it would be premature to look at further expanding the remit or scope of this legislation. In addition, with an existing review of the *Privacy Act 1988* underway, obligations to enhance protections over customer data and the systems that house these may be more relevant to include within these legislative updates.

The SOCI reforms, through the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI) and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP), present a significant uplift in legislative obligations on a widened range of critical infrastructure sectors. Whilst some obligations are already in place, such as the requirements to register critical infrastructure assets and mandatory cyber incident reporting, many of the expansive obligations associated with maintaining a Critical Infrastructure Risk Management Program (CIRMP) are still being implemented by critical infrastructure providers targeting compliance by the due date in August 2023. Beyond this, the first Annual Report from the Board of critical infrastructure providers is not due until September 2024.

Further reforms to this legislation such as including customer data in reference to 'critical assets' will further extend the number of sectors and critical infrastructure providers that will be captured under this legislative regime. Given the increased number of sectors captured under the existing reforms, in addition to the raft of new critical infrastructure assets that the Department of Home Affairs and Australian Cyber Security Centre (ACSC) will need to become familiar with, there may be challenges in the government's ability to effectively monitor and regulate further broadening of the scope of this Act.

In addition, improvements to the security and resilience of critical infrastructure assets associated with SOCI are not yet being realised due to the current timeline for compliance with the CIRMP. With limited visibility of the enhanced security outcomes associated with the reforms of the Act to date, it is difficult to conclude that further expansion of this legislation is likely to derive the outcomes Government is seeking to achieve through any further amendments. A more prudent approach should be to properly embed the existing reforms, assess the actual regulatory impacts associated with these reforms being put into practice, and then make determinations as to what (if any) further SOCI amendments are required.

Finally, it is recognised that following the Optus, Medibank and Latitude data breaches, there were limitations in the extent to which Government was able to intervene under the existing legislative landscape. These data breaches have triggered a heightened focus and prioritisation in driving the legislative changes to the Privacy Act, and it is suggested that this may be the most appropriate avenue to look at expanding obligations associated with protections over customer data and associated systems.

2c. Should the obligations of company directors specifically address cyber security risks and consequences?

Directors are currently subject to a mix of principles-based and specific obligations. Any new obligations which are introduced may displace the focus applied to existing duties and obligations, so they need to be carefully considered. They must also take into account the relevance of cyber security to different industries; those with a limited customer-facing footprint will handle less sensitive data and thus should have less onerous requirements than large customer-facing organisations which hold large quantities of personal and sensitive data.

There are obligations which, in some settings, already have the effect of requiring Directors to specifically address cyber security risks and consequences. These include *CPS 234 Information Security*, which identifies the Board as ultimately responsible for the information security of an APRA-regulated financial institution. The *Security of Critical Infrastructure Act*, which applies to a much broader range of organisations, will also require increasing awareness and reporting of cyber incidents.

To effectively oversee cyber security risks, Directors should be expected to possess a baseline level of cyber security literacy. This enables them to better understand and oversee the management of cyber security risks, while also fostering a culture of security awareness within their organisations. There is precedent for Directors' obligations and penalties to be specific, such as those relating to providing a safe workplace and ensuring the payment of PAYG Withholding tax, GST and Superannuation. However, the nature of cyber threats and vulnerabilities is changing, and the exposure of different industries to a cyber-attack must be taken into account. Broad obligations may be more appropriate in these circumstances; any additional obligations should be targeted at awareness, rather than requiring a detailed understanding of threats or vulnerabilities.

In conclusion, there are several legislative and regulatory instruments through which cyber security related obligations are already placed on Directors. We are supportive of further obligations to capture other high-risk industries, however these obligations must be considered in totality with existing

obligations and must be sufficiently flexible to not place an administrative burden on organisations with a low inherent risk of being subject to a cyber-attack.

2e. 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 operating environment for many sectors across Australia is becoming increasingly complex, and regulatory compliance is a significant risk to a significant volume of corporate boards. Part of the complexity occurs due to the increasing disconnect between Federal, State, and Sector-specific regulation.

The Federal Government should take a lead in addressing this public policy problem and driving more robust assessment of existing regulation and engagement with relevant regulators. Protocols should be established for how duplicative or conflicted regulatory requirements should be navigated.

2f. 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 US Treasury Department's Office of Foreign Assets Control has warned of potential penalties for permitting the payment of ransoms by cybercrime victims, and some US States have introduced prohibitions on these payments. While this has been done in an attempt to undermine the business model of these cyber criminals, data is too recent to determine if this has had a material effect on the prevalence of attacks or ransom payments. The decision to criminalize the payment of ransoms also has several drawbacks:

a) Victims of cybercrime may refrain from reporting or disclosing information about the threat of cyber extortion to law enforcement authorities or regulators out of fear of facing punitive or criminal consequences (both legal and financial).

b) Prohibiting the payment of ransom only deals with one motivating factor for cyber criminals, which is financial gain. Motives for cyber-attacks can also be ideological (religious or political), revenge or humiliation (personal or professional).

c) Attackers may not be aware of a nation's extortion payment prohibition. With the increasing popularity of ransomware kits (Ransomware-as-a-Service) sold on the dark web for as little as $50USD, attacks may be executed with little planning or premeditation.

d) While the average ransom paid to cybercriminals decreased by 34% from Q4 2020 to Q1 2021, the number of cyber-attacks has continued to rise year on year. It is estimated that a company is faced with a ransomware attack every 11 seconds. Therefore, it is questionable whether criminalizing ransom payments by organisations would have a significant impact on the frequency of cyber-attacks.

e) Civil penalties may not deter a business in paying ransom if the cost of the civil penalty can simply be absorbed when faced with the very survival of the business itself.

f) Due to their nature, cyber criminals usually demand ransomware payments be made outside of the legitimate banking system, via cryptocurrency. This would make tracking and enforcement of such a prohibition very difficult.

On the basis of these considerations, we support the Government in publicly discouraging the payment of ransoms, however we do not support the criminalisation of their payment.

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?

In theory it makes sense to have a level of separation between the ACSC, who wish to work collaboratively with organisations to mitigate cyber incidents, and the various industry regulators who seek to enforce laws and regulations. However, in practice we believe that an explicit confidentiality obligation would not be helpful.

There are likely to be cases where the ACSC needs to share information with regulators and other agencies, for example to mitigate serious harm to individuals who have been implicated in a cyber incident. This is analogous to how healthcare professionals need to balance obligations for patient confidentiality with obligations to report suspected illegal activity.

In our experience, the vast majority of organisations want to do the right thing and comply with the law. In fact, organisations with formal risk appetite statements usually have a very low tolerance to non-compliance with the law. Organisations who fail to report incidents to the relevant regulators usually do so out of a lack of awareness rather than reluctance. As such, in our view it is unlikely that organisations are avoiding engagement with the ACSC out of fear of regulatory action. However, if the government pursues a strategy of imposing significant financial penalties for voluntarily reported incidents, such as with the *Privacy Act* amendments, then this may change.

In addition to the above, particularly when it comes to data sharing and surveillance, and promise of confidentiality will likely be met with scepticism. Developments over the past years have contributed to such scepticism, including for example the Robodebt scandal that involved cross-agency data matching, elements of *The Assistance and Access Act* that would have required encryption backdoors, and the Snowden leaks that revealed that the ASD was implicated in mass surveillance activities.

In conclusion, we believe that an explicit obligation for confidentiality is not necessary given that there may be a legitimate need for the ACSC to share information with other agencies and regulators, that organisations are not intentionally avoiding informing regulators, and that regardless of these factors, any promise of confidentiality would likely be met with scepticism.

9. Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Currently, organisations are required to notify the ACSC of such incidents and the affected asset/infrastructure. In the instance of a data breach, the data breach is also included as part of the notification, under the Notifiable Data Breaches Scheme. Expanding the regime of cyber security incident notifications would indeed assist in improving the public understanding of ransomware and extortion. Exposing the public to more information on the cybercrime environment should translate to greater awareness and fewer incidents.

Expanding the regime beyond its current state could require additions such as mandatory reporting of extortion demands received from ransomware attackers, suspected method of attack and deadlines/timelines in which to deliver on attackers' demands. From a public perspective, having access to this information will gradually result in a population that is better informed of the threat landscape. This will enable them to better identify the areas in their personal and work lives that are potential weaknesses for ransomware attackers. In addition to understanding individual areas of weakness, information surrounding extortion demands and deadlines given by attackers should improve understanding surrounding the type of scenarios faced within a ransomware incident. This will allow individuals to bolster responsive, detective and preventative controls against ransomware attacks in a personal and professional context.

11, 12. [Combined] Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

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

With a growing demand for workers in the cyber security industry, analysts have forecasted 30,000 unfilled jobs in Australia by 2026 and a global projection of 3.5 million unfilled jobs by 2025. Though broader Government STEM programs are relevant to this increasing demand, this may be insufficient to specifically uplift cyber skills.

Over the last decade, the world has been witnessing a rapid increase in cyber-attacks, with approximately 80% of them because of human error. In addition to a shortage of cyber security professionals, this has brought to light the increasing need for workforce-wide cyber security awareness training and upskilling. The Australian government can provide support by implementing several activities that would enable organisations to prepare for cyber threats proactively.

- Subsidise Cyber Security Training: Government should provide specific incentives for students or existing professionals to study cyber security degrees and accreditations, such as scholarships and grants. This would be similar to schemes which have been applied to other areas of skill shortage, such as for nursing studies in Victoria. Subsidies help to reduce the financial burden of obtaining training, which can be particularly beneficial for smaller businesses or individuals with limited financial resources, such as high-school leavers. This would increase the national pipeline of cyber security professionals and national cyber resiliency in the prevention of cyber-attacks and data breaches. Subsidies could be applied to TAFE and University courses, as well as cyber security accreditations such as Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA).

- Incorporate Cyber Security into a Broader Range of Degrees: Current career paths within cyber security are heavily focused on more technical areas of the industry, such as penetration testing. Most, if not all, cyber security degrees or subjects sit within Computer Science, Programming, Engineering, and IT faculties. This fails to provide the tools and cyber skills to individuals that go into the workforce outside of the technology industry. There is an opportunity for universities to incorporate cyber security related courses into existing degree courses which would fit the needs and skills required for those fields. For example, offering Risk Management courses for Business Degrees, Counterterrorism & Cyber Security Courses for Political Science or Security studies, and Cyber Security & Anti-Money Laundering courses for Business & Finance Degrees.
- Reduce Barriers for Overseas Cyber Security Skilled Immigration: Data shows that cyber security professionals are the sixth most in-demand category of technology professional in Australia. An urgent focus on closing the national skills gap should see the invitation and support of introducing new immigration visas, similar to the abolished 457 visa, to counter the limited national availability of cyber security professionals. Such a visa would encourage skilled workers within the field to immigrate and grow the skilled workforce within Australia.
- Implement a Standardised Role Framework: Australia should model the US National Initiative of Cyber Security Education (NICE) Program to define cyber security roles based on the skills, knowledge and tasks needed to perform them. The framework would be a key pillar in the development of cyber resiliency within industry wide workforces by engaging in learning activities to develop their knowledge and skills. As with the NICE framework, the framework can be divided by audience, such as for employers, educational providers and individuals. Each audience section includes listed resources with materials aimed at helping its audience in building materials, measure, assess, and build their cyber security workforce or career path options. Rather than creating a separate program, the ACSC could develop such a framework.

In conclusion, the Australian government can support organisations by providing subsidies for cyber security accreditation, promoting cyber security events and information sharing platforms, supporting new cyber security degrees and courses, reducing barriers for overseas cyber security skilled workers immigrate, and implementing a standardized framework to define cyber security roles. By doing so, Australia can create a culture of cyber resilience and proactively prepare for cyber threats.

13a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The *Security of Critical Infrastructure Act* was amended to introduce mandatory cyber incident reporting obligations for specified critical infrastructure entities to Commonwealth entities, including the ACSC. Critical cyber incidents must be reported within 12 hours from the time that an organisation becomes aware of them, and other incidents within 72 hours. APRA regulated institutions must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident. Other reporting requirements are varied in the depth and timeliness of information required.

We support harmonisation of reporting requirements, including the classification of cyber incidents and associated reporting timeframes across regulators, to:

- Provide greater clarity for organisations and consistency in timely and accurate reporting of cyber incidents;
- Expedite the Government's ability to identify, investigate and respond to cyber incidents through greater transparency and better coordination across regulators and impacted organisations; and
- Increase the Government's ability to identify and analyse systemic issues, threat activity trends and emerging cyber risks resulting from isolated incidents, and to more enable more effective cyber threat response plans and actions.

14. What would an effective post-incident review and consequence management model with industry involve?

Post-incident reviews are an important part of identifying and understanding the root cause of an incident and to prevent similar incidents from re-occurring in the future. The Government or a regulator could establish clear guidelines for the minimum requirements for organisations when conducting post-incident reviews. This could include a review of the effectiveness of the control environment of an organisation, inclusive of third- and fourth-party systems and services.

Regulated financial services entities are currently required to manage cyber security risk in accordance with *CPS 234 Information Security*. Penalties for non-compliance with this standard and broader risk management standards can result in capital overlays, Enforceable Undertakings, and ultimately a loss of licence. This appears to be effective, with a high awareness of CPS 234 and compliance requirements among the Directors and staff of regulated entities.

A consequence management framework applied to cyber risk requirements for a broader range of Australian organisations would aid as a strong incentive to manage this risk effectively.

15a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

We see the following opportunities for the government to support in assisting small businesses in mitigating and managing their cyber risks:

- Subsidise Cyber Security Software Solutions: Cyber security software is often overlooked and disregarded by most small to medium organisations. This is due to lack of awareness of the threat environment and a generally low appetite for the ongoing cost of such services. It would be in the interest of the government to partner with cyber security protection providers to subsidise these services for small businesses. This would make such services more accessible and ultimately uplift cyber resiliency across the small business sector.
- Conduct Broader Awareness Exercises: The ACSC provides useful information on reducing personal cyber security risk. It also includes broader information on cyber security programs and recent vulnerabilities. However, this content requires a user to seek it and awareness of the ACSC among the general public is low, particularly for vulnerable groups (such as the elderly). A much more prolific and broader range of marketing and advertising exercises should take place to make individuals and businesses aware of this content.

Conclusion

Thank you for providing us with the opportunity to provide input into this discussion paper. Please feel free to contact us to discuss any of these items in further detail.

Sincerely,

Amstelveen
Email: info@amstelveen.com
Address: Level 11, 570 George Street, Sydney NSW 2000
Web: https://www.amstelveen.com

Our Authors

David van Gogh
Director

David has 15 years of experience in technology, projects and governance, spanning risk advisory, compliance, internal audit, corporate governance, risk remediation, risk culture and the delivery of major technology and business change projects. His experience is concentrated in heavily cyber-risk engaged industries, such as financial services and telecommunications.

Louis Wellard
Director

Louis has 15 years of risk management experience spanning risk, controls, corporate governance, regulatory compliance, project management and program governance. He has worked with a range of clients across Australia, New Zealand, the broader Asia Pacific and South America, including specifically on the implementation of the SOCI Act.

Andrew Millward
Director

Andrew is a technology risk and information security professional with 12 years of experience in risk management, internal audit and information security. He has worked in a variety of roles advising and supporting risk management functions, internal audit, project teams, steering committees and project sponsors of large Australian corporations.

Romana Bizjak
Director

Romana is a risk and compliance professional with 15 years of experience across the financial industry. She has specific experience with cyber risk in a financial services context and has advised on methodologies for the assessment of cyber risk and controls, performed cyber risk assessments for critical banking services, and led large risk and compliance uplift programs.

Emma Fabreguette
Consultant

Emma is a risk, cyber security and technology specialist with her experience concentrated in industries with a high exposure to cyber risk, such as financial services and aviation. She contributes to cyber-related public policy, has worked with the Israeli International Institute for Counter-Terrorism and is a member of University of Chicago's Young Leaders in Cyber security.

Brandon Nguyen
Consultant

Brandon is a risk, compliance and legal specialist with strong experience in risk and control management. This experience includes work in major financial institutions with a heavy exposure to cyber risk, such as superannuation, private equity and venture capital.

Kenneth Chu
Consultant

Kenneth is a risk and compliance management professional with a background in finance and business. Kenneth has worked with Amstelveen's clients in the banking and insurance industries on technology and operational risk and compliance matters.

Sri Narain
Consultant

Sri is a risk and compliance management professional with a background in finance, economics and financial risk management. Sri has worked with Amstelveen's clients in the banking and telecommunications industries on technology and operational risk and compliance matters.