13 April 2023

2023-2030 Australian Cyber Security Strategy
Expert Advisory Board
Department of Home Affairs

Via: Home Affairs submission form

Dear Board

2023-2030 Australian Cyber Security Strategy Discussion Paper

Chartered Accountants Australia and New Zealand (CA ANZ) welcomes the opportunity to contribute to the Expert Advisory Board's discussion paper noted above. With over 135,000 members around the world, in government, academia, large and small businesses, our members are well placed to contribute to keeping critical data and systems secure. Our members in public practice are also in an ideal position to support the government's aim of raising community awareness on how to make cyber-aware choices. Appendix B provides more information about CA ANZ.

Broadly, we support the four cornerstones for a forward-looking strategy, that is, a strategy that is enduring, affordable, achievable and flexible. We consider these cornerstones fundamental in light of the Government's goal to become 'the most cyber secure nation by 2030'.

We recommend that the following be key considerations when developing the Strategy:

- Providing guidance in plain language as well as industry terminology.
- Creating a single door for Australians to find:
    - guides on how to be cyber safe;
    - the obligations for those that collect and retain critical data; and
    - how to access help if a victim of cyber-attacks.

We provide the following feedback on those areas raised in the paper where we consider we can add the most value in Appendix A. We will continue to support our members to implement strategies to mitigate cyber-attacks with tools such as our CA Cyber Security Playbook and Baseline Cyber security checklist. These tools are available to be shared with clients of our members to raise the importance of cyber security in the community.

We would welcome working with the Government on specific initiatives that can be disbursed through our member network. Please do not hesitate to reach out for further discussion, in the first instance, to Karen McWilliams on [redacted] or at [redacted]

Sincerely,

[redacted]

Simon Grant FCA
Group Executive
Advocacy & International Development

Appendix A

We provide the following feedback on areas where we consider we can add the most value.

Enhancing and harmonising regulatory frameworks

As the Government heard, business owners 'do not find their cyber security obligations are clear or easy to follow.'[1] This reflects the findings of the *2021 State of Cyber Fitness in Australian small businesses white paper (White Paper)* which found 'advice from experts is often inconsistent and generalised, creating confusion and, at times, apathy'. While more explicit specifications may be helpful, it is more important that the Strategy uses plain language rather than industry terminology when seeking to convey the importance of protecting customer data and how best to do so.

We also encourage the Government to take any opportunity to streamline the existing framework. As referred to in our submission 2022 to the National Data Security Action Plan, there were 9 Government agencies at the Federal level with varying roles and responsibilities, fulfilled through 14 Government mechanisms. Equally, as the Counts of Australian Businesses from the Australian Bureau of Statistics at June 2022 shows, the majority of Australian businesses are sole traders and micro businesses (31 per cent are sole traders and a further 28 per cent employ less than 5 people).

A single legislative framework with obligations scalable to the size of the entity is critical when considering the findings of the White Paper found that the 'smaller the business the more likely day-to-day IT tasks will be managed by the owner.'[2]

For example, it may be reasonable to require large businesses to meet a cyber security standard while requiring sole traders, micro and small businesses to undertake a periodic government-funded cyber security health check. Alternatively, requirements could be scaled according to activities undertaken. For example, entities storing customer data could be required to meet a cyber security standard, while those who have one-off interactions with customers, such as a sale online, to undertake a periodic government-funded cyber security health check.

When considering the potential for a new *Cyber Security Act*, we consider it critical that it does not add to the already significant existing legislative framework for business. As raised in our submission in 2021, businesses are managing a diverse range of risks, and it is important for cyber security governance to fit within these wider considerations. Equally, as cyber security risks do not necessarily correlate with entity size, the Government will need to take a nuanced, rather than one-size-fits-all, approach.

In particular, the Government should identify those existing legislative instruments which would be repealed on the introduction of a proposed *Cyber Security Act*. Obligations on entities under a new *Cyber Security Act* would need to be appropriately scalable for entities of different sizes.

Australia's regulatory framework must aim to streamline obligations, and tools to meet those obligations, and be appropriately scalable for and understandable by business owners of all sizes of entities.

[1] 2023-2030 Cyber Security Strategy Discussion paper, December 2022, page 17
[2] Big cyber security questions for small business, 2021, page 14

Securing government systems

To question 6 of how the Government can demonstrate and deliver cyber security best practices, we refer to initiatives in the United Kingdom. The National Cyber Security Centre (NCSC UK) in the United Kingdom is exploring providing access to private entities for the cyber defence services it has developed for use by government agencies. Under current consideration is access to its "Protective Domain Name Service" currently able to be deployed by certain public sector agencies[3] and "Check your cybersecurity[4]" free government service for UK to identify common vulnerabilities in public-facing IT of an entity.

As the Government enhances its cyber posture, consideration should be given to providing private sector access to the tools deployed. This would provide a trusted source of tools to combat cyber-attacks and incentivise Australians to improve their own cyber security. Especially as the baseline for cybersecurity is shifting constantly due to threat complexity and the advent of new technologies. These baseline requirements are becoming a non-negotiable fundamental for a business to remain viable alongside cash flow and profitability.

The Australian Cyber Security Centre's (ACSC) 2022 Annual Cyber Threat report also indicates that small to medium businesses (SMBs) are being increasingly targeted by threat actors. The report also mentions a concerning global trend that state actors are also increasingly targeting the SMB's although that trend is yet to be seen in Australia. The report also states that there are 150,000 to 200,000 Small Office and Home Office (SOHO) routers that are vulnerable. It is therefore fundamentally important that a national set of tools are publicly accessible and their availability promoted often to enable these vulnerable SOHO businesses, which do not have the cash flow and purchasing power of large enterprises, to implement baseline cyber security.

Improving public-private mechanisms for cyber threat sharing and blocking

We strongly support the Government sharing intelligence on emerging threats and harnessing existing business networks, such as our members in public practice, to distribute such intelligence. Importantly, when sharing such knowledge, it must be coupled with the practical steps non-cyber experts can take to mitigate the latest type of attack.

Community awareness and victim support

We welcome the opportunity for the Strategy to invest further in building cyber security skills and raising community awareness. We favour the Strategy prioritising raising community awareness over building skills as there is no motivation to take action to protect your data from a threat you are not aware exists.

As recommended in our Federal Budget Submission in January 2023, we consider the first step is a paid marketing campaign that promotes the value of being cyber-secure and the tools and resources produced by the ACSC to become cyber-secure. Such a campaign should be run regularly to reach the owners of the more than 400,000 businesses started each year and to convey emerging threats.

As an accredited tertiary education body, CA ANZ supports building cyber security skills though cautions that the Strategy must recognise that not all Australians have access to the resources, or have the interest, to gain such skills. For example, sole traders and owners of small businesses must direct their resources to run their businesses and would rely heavily on buying a software solution or engaging an expert to ensure cyber security.

In tandem with building skills, the Strategy could consider providing a vehicle for Australians to identify reputable and trusted service providers and products. We refer again to initiatives in the United Kingdom where the NCSC UK provides a "Verify a Supplier tool"[5] on their website. Providers are assessed against NCSC standards and, if certified, can apply the NCSC brand.

---

[3] NCSC's Protective Domain Name Service, https://www.ncsc.gov.uk/information/pdns, last accessed 5 April 2023
[4] NCSC's Check Your Cyber Security Service, https://checkcybersecurity.service.ncsc.gov.uk/, last accessed 12 April 2023
[5] NCSC's Verify a Supplier, https://www.ncsc.gov.uk/section/products-services/verify-suppliers, last accessed 5 April 2023

Such a tool could capture cyber-security consultants, software applications that provide cyber security and the manufacturers of products used by consumers to capture, transfer and store critical data. Where such products meet defined standards, they can apply ACSC branding. We reiterate our recommendation in our submission in 2022 that the burden of applying expertise to make data holding secure should be placed on those best resourced to do so, the manufacturers.

A precedence for the Government to provide a trusted list of suppliers is the Australian Taxation Office (ATO) Software Solutions for Single Touch Payroll.[6] The ATO assesses software solutions against three criteria and if met, publishes them on its site. Of relevance to cyber security solutions, is the criteria that the solution must not require the employer to maintain the software.

The strategy should also seek to provide information in a wide variety of forms with a broad variety of case studies. This would address the findings of the White Paper that business owners seek '*targeted recommendations that speak to their specific circumstances. …Checklists and case studies focused on their industry and business size were suggested as one way to address this problem*.'[7]

Critically, raising awareness, building skills and victim support should be seen to come from a single Government source. We consider a key aim of the Strategy will be to provide a single portal for the community to find practical steps to be cyber-secure, examples of cyber security best practices, report cyber-attacks and access support if a victim of a cyber-attack. Once through the door, to allow the user to personalise their pathway and find, for example, information in plain language and case studies specific to their industry sector.

[6] Australian Taxation Office, https://www.ato.gov.au/Business/Single-Touch-Payroll/In-detail/Software-solutions-for-Single-Touch-Payroll/, last accessed 5 April 2023
[7] Big cyber security questions for small business, 2021, page 34

Appendix B

Chartered Accountants Australia and New Zealand (CA ANZ) represents more than 135,000 financial professionals, supporting them to build value and make a difference to the businesses, organisations and communities in which they work and live.

Around the world, Chartered Accountants are known for their integrity, financial skills, adaptability and the rigour of their professional education and training.

CA ANZ promotes the Chartered Accountant (CA) designation and high ethical standards, delivers world-class services and life-long education to members and advocates for the public good. We protect the reputation of the designation by ensuring members continue to comply with a code of ethics, backed by a robust discipline process. We also monitor Chartered Accountants who offer services directly to the public.

Our flagship CA Program, the pathway to becoming a Chartered Accountant, combines rigorous education with practical experience. Ongoing professional development helps members shape business decisions and remain relevant in a changing world.

We actively engage with governments, regulators and standard-setters on behalf of members and the profession to advocate in the public interest. Our thought leadership promotes prosperity in Australia and New Zealand. Our support of the profession extends to affiliations with international accounting organisations.

We are a member of the International Federation of Accountants and are connected globally through Chartered Accountants Worldwide and the Global Accounting Alliance. Chartered Accountants Worldwide brings together members of 13 chartered accounting institutes to create a community of more than 1.8 million Chartered Accountants and students in more than 190 countries. CA ANZ is a founding member of the Global Accounting Alliance which is made up of 10 leading accounting bodies that together promote quality services, share information and collaborate on important international issues.

We also have a strategic alliance with the Association of Chartered Certified Accountants. The alliance represents more than 870,000 current and next generation accounting professionals across 179 countries and is one of the largest accounting alliances in the world providing the full range of accounting qualifications.