Tech Council

21 April 2023

Department of Home Affairs
auscyberstrategy@homeaffairs.gov.au

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper

Thank you for the opportunity to provide input on the 2023-2030 Australian Cyber Security Strategy. The new strategy is one of the highest priorities for the Tech Council and its members. We have brought together a dedicated 'tiger team' of multidisciplinary experts from across our membership to help identify solutions for the Government's consideration, and to improve industry-government collaboration to lift Australia's cyber resilience.

About the Tech Council of Australia (TCA)

The TCA is Australia's peak industry body for the tech sector. The Australian tech sector is a pillar of the Australian economy, contributing $167 billion to GDP per annum and employing over 860,000 people. This makes the tech sector equivalent to Australia's third largest industry, behind mining and banking, and Australia's seventh largest employing sector.

The TCA represents a diverse cross-section of Australia's tech sector, including leading Australian software-as-a-service companies, multinational companies, fintechs and venture capital and investment advisory firms.

Executive Summary

The Tech Council strongly supports the development of a comprehensive new cyber security strategy and the Government's ambition to become the world's most cyber secure nation by 2030.

The strategy is firstly an opportunity to identify and quantify the types of cyber threats and risks Australia will confront and the vulnerabilities they will try to exploit. This will help concretely frame Australia's task to keep its citizens and businesses secure.

It is also an opportunity to develop a holistic government, economy and society-wide response to cybersecurity, which leverages the full suite of policy levers across government to help lift our cyber preparedness and resilience as a nation.

It is finally a chance to prepare for the technological advances that will shape the cyber landscape over the period from now to 2030, to enhance the culture of collaboration and cooperation between government, industry and the community, and to take a best practice approach to regulation.

We recognise that the Government is drafting this strategy in a fiscally constrained environment but believe there are significant opportunities to leverage existing programs across Government, combined with regulatory reforms.

We have developed this response building on our Tech Council white paper, roundtables with the Department of Home Affairs and the Expert Panel, as well as the valuable input and expert contributions from our member company community. We address the three 'core policy areas' as well as the seven 'areas for potential action' outlined in the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

In summary, our priorities for the cyber security strategy include:

- A **regulatory reform agenda that is risk-based, focused on simplification, clarification, and incentivising good behaviour**. This should be underpinned by an audit of the of existing regulation in the landscape and coordinated with other reform processes across Government. This includes privacy, digital identity, electronic surveillance and e-safety. Our key priorities for reform include governance and administration, reducing overlap and duplication, and improving standards and incentives – all aimed at making our cyber security framework more responsive, agile, and effective.

- A **collaborative approach to working with industry on secure software development** which prioritises international interoperability and harmonisation on standards and recognises the shared responsibilities for cyber security across the supply chain. We welcome ACSC's involvement in the multilateral process for secure-by-design and -default guidance. However, we do not support any immediate moves to regulate secure-by-design and -default requirements or mandate secure software development standards given they remain relatively immature and lack the necessary standards infrastructure at the present time, but would welcome an opportunity to engage with the Government on alternative models to drive engagement and uptake of these standards in the Australian tech sector, and to participate in cost-benefit and regulation impact analysis processes for any future regulatory proposals.

- A **concerted focus on building Australia's cyber and tech workforce**, including an overhaul of the skilled migration system, new pathways for skilling and reskilling such as digital apprenticeships, embedding cyber across the education system, and improving diversity in the cyber/tech workforce.

- **Growing Australia's cyber security industry** capabilities, particularly by addressing funding gaps and market failures in venture capital investment by leveraging the National Reconstruction Fund and improving administration of the Foreign Investment Review regime.

- Promoting **technology innovation and adoption** that can help prevent or reduce the impact of successful cyber-attacks, including by expanding the trusted digital identity framework across the economy and developing a plan for post-quantum cryptography, starting with sensitive government datasets.

- Introducing a more **formal and structured national response and review framework** for major cyber security incidents, which could be led by the new National Coordinator and Office for Cyber Security (backed by appropriate statutory powers).

- **Enhancing public-private partnerships on threat sharing and blocking**, including by improving two-way sharing of information and intelligence, adopting sophisticated partnership models (including on Secure G), and improving administration of threat sharing architecture taking account of international best practice.

Tech Council

1. Introduction: A Tech Sector Perspective on Cyber Security in Australia

The recent high profile data breaches, combined with the rise of emboldened state-based actors, warrants a comprehensive and collaborative response that unites government and industry to improve our national cybersecurity readiness and resilience.

Australia is a wealthy, educated, advanced economy with some of the best tech talent in the world, a rapidly growing tech sector and tech-savvy consumers that are early adopters of new technology. We have the right foundations for a world-class cyber security environment, and we can continue to work to improve coordination, as well as increase the effectiveness of our prevention and post-incident response mechanisms. Importantly, there is much more work to do to grow our cyber industry workforce and ecosystem.

The most recent cyber threat reporting from the Australian Cyber Security Centre (ACSC) is just the latest in a series of assessments demonstrating the burning need to improve our cyber resilience. This goal isn't just critical to our national security, it is also central to our economic security and the growth of our digital economy.

Improving Australia's national cyber security posture isn't just a matter of national security. As we transition to a highly digitised and interconnected tech environment, cyber security will be a fundamental underpinning to our economic strength and social stability. The 2030 strategy presents an opportunity to broaden our perspective to create a truly whole-of-government, economy, and society response to cybersecurity, which includes leveraging the full suite of policy levers across government. We believe that there are four essential components to getting us there:

1. A clear national cyber security plan underpinned by effective coordination between the public and private sectors (from threat intelligence sharing to post-incident response and assessment);
2. Creating a strong pipeline of cyber and tech talent, a thriving Australian cyber and tech ecosystem, and an uplift in cyber capabilities across the economy (including in small businesses and individuals);
3. Better use and adoption of technologies that can help prevent or reduce the impact of successful cyber-attacks, such as digital identity, 2FA/MFA; and,
4. A modernised legal framework fit for the digital age that creates the right incentives for organisations to invest in the appropriate collection, use, protection and decommissioning or deletion of data, personal information and systems.

Becoming a world leader in cyber security – underpinned by a thriving tech workforce and ecosystem – can provide Australia with a competitive economic advantage, underpinning our shared effort with the Australian Government to reach 1.2 million tech jobs and increase the tech sector's economic contribution to $250b annually by 2030.

2. Key considerations in developing the cybersecurity strategy

We strongly encourage the Government and the expert panel to take account of the following four guiding principles when finalising the new cyber security strategy.

2.1 A more holistic approach to cyber security uplift

While Government systems and capabilities should be a core component of any Australian Government cyber security strategy, it is also important to recognise that cyber security is a whole-of-society challenge that necessitates a broader approach.

The conventional conceptualisation of cyber security in recent years has been that we need to 'keep the bad guys out'. The current conceptualisation of the problem is too narrow and leads to an overly specific focus on offensive and defensive cyber capabilities. Yet, Australia is not an island in cyberspace and there are important and often simple steps that can be taken by organisations and individuals to improve their cyber preparedness and resilience. We need to shift towards a more holistic approach to cyber security that encompasses businesses and individuals across the economy and supports them to better manage cyber risks by implementing good cyber hygiene, security and privacy practices.

This needs to include broadening cyber messaging beyond a focus on technical controls and technology, to helping businesses and individuals understand the critical role of people and process in improving cyber resilience and preventing data breaches. We won't improve whole-of-nation cyber-literacy and long-term behavioural change if there is an ongoing perception of cyber security being the domain of technology experts.

This includes consideration and better awareness of risks associated with trusted insiders, human error, as well as data management and storage (noting Government can do more to issue guidance on proven practices in data management, storage, and data deletion which would help organisations reduce their sensitive data "footprint", which would reduce the impact of a successful cyber-attack).

2.2 Adopt a future-forward perspective that prepares Australia for a rapidly evolving threat landscape

We need to simultaneously better position Australia to adapt to technologies that are reshaping the current cyber landscape, while preparing for emerging technologies on the horizon. While these technologies can improve how we prevent and respond to cyber incidents, they can also be used by bad actors in ways that create new vulnerabilities.

In the near-term, there needs to be greater recognition and awareness of the cyber vulnerabilities that are created in government and across the economy from using legacy IT systems and software. Many of these systems are often outdated and not designed with modern cybersecurity threats in mind which increases their vulnerability. The need for digital transformation in Government and the broader economy is essential to bolster cybersecurity.

Artificial Intelligence is also presenting new cyber security challenges from phishing, fraud and scams at speed and at scale. Inversely, having the potential to identify patterns and anomalies in data via AI can help improve the ways we learn and adapt at the rate we need to keep pace with evolving cyber threats (while staying clear-eyed about the limitations).

Quantum computing is also expected to have a major impact on cyber risk by breaking some forms of encryption and weakening others. However, it also presents significant advantages to increase cyber security through the use of quantum cryptography, for example. We need to start preparing for the era of by continuing to invest in and implementing quantum-resilient cyber security measures while also growing Australia's quantum ecosystem.

While these technologies won't be a panacea to solving cyber security problems, we need to ensure that we stay ahead of the curve to leverage the best of these technologies to remain resilient.

2.3 Fostering a better culture for cooperation and coordination within government, as well as across industry and the broader community

Cooperation between Government and industry needs to be enhanced across the full spectrum of activities, from threat intelligence sharing to post-incident response and assessment. Improved mechanisms for cooperation and coordination helps us design for a more trusted digital ecosystem and positions us to make our people a cyber asset, rather than a cyber vulnerability.

Greater cooperation on activities that can prevent or minimise cyber incidents, such as sharing of threat intelligence, is seen as particularly valuable by industry to improving cyber security. There is significant room for improvement in the current ACSC mechanisms to enable sharing of threat intelligence.

Just as importantly, the current models for preventing, disclosing, coordinating and collaborating around cyber-attacks need to be reviewed and enhanced given the intensifying threat environment and emerging evidence of policy gaps and issues. Consideration should be given to identifying a single controller and establishing a more coordinated operational model for incident handling by government agencies, as well as a more formal mechanism to review lessons learnt from cyber security incidents to prevent recurrence of past mistakes. Efforts should also be made to reduce overlapping reporting and regulatory requirements across government to streamline the system and make it work more effectively.

2.4. Best practice regulation of the digital economy

Finally, while we support regulatory reform as being a core part of the strategy, we recommend the Government adopt an overarching approach that is guided by clearly articulated principles for best practice regulation of the digital economy:

- Informed and coordinated – underpinned by rigorous analysis and industry engagement, with thoughtful consideration of the interrelationships with other policies and regulation, such as privacy, digital ID, electronic surveillance reform and online safety
- Proportionate – taking a risk-based approach targeted at addressing clearly defined problems and gaps
- Timely – responsive to the changing threat environment and cautious in moving too far ahead of overseas jurisdictions in a way that could jeopardise Australian industry
- Consistent and interoperable – including with global and domestic regulation to improve the ease of doing business and maintain Australia's investment attractiveness; and
- Has a bias to innovation and growth – including by avoiding prescriptive technical requirements that may quickly become outdated or inhibit innovation, and by enabling new technologies that can help improve the risk environment (e.g. digital ID) to provide Australia with a competitive advantage in the digital age.

3. Response to Core Policy Areas

3.1. Legislative and Regulatory Reforms

3.1.1. Moving towards a clearer, more streamlined and effective cyber regulatory framework

We support the Government's and the expert panel's focus on best practice regulatory reform to ensure our laws and standards are fit for the digital age, and to improve the incentives for businesses to adopt better cyber security practices across the nation. We start from the position that simplification, clarification and incentivising good behaviour needs to be the primary

objective of the regulatory reform agenda, given cyber security regulation is already a complex and crowded space.

According to previous research by the Department of Home Affairs, there are "at least 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses"[1]. Moreover, the Government currently has multiple reform processes underway that have some relevance to addressing cyber security or related risks:

- Cyber Security Strategy and SOCI risk management reforms
- Privacy Act Review (building on recent reforms to the penalty regime)
- Digital identify reform
- Electronic surveillance reform
- Online Safety Act implementation (industry codes)

There are also multiple agencies with some level of responsibility for cyber security regulation, compliance, enforcement and response. At the federal level alone, this includes Home Affairs, Australian Signals Directorate, Australian Cyber Security Centre, Department of Defence, Attorney-Generals Department, Office of the Australian Information Commissioner, Australian Federal Police, Australian Communications and Media Authority, Australian Securities and Investments Commission, Australian Prudential Regulatory Authority, eSafety Commissioner and more. This doesn't take into account the interests of other federal departments in cyber security policy, and the many state and territory agencies that have an operational role.

To help design the regulatory reform agenda and determine whether to proceed with an entirely new Cyber Security Act or utilise existing legislation, we recommend the Government commission an audit of existing laws and regulations to help identify gaps, overlaps, duplication or conflicting requirements. We also recommend the adoption of overarching objectives and principles to ensure a coordinated and coherent approach to reform across the multiple reform processes currently underway.

Notwithstanding these recommendations, we have also identified three key areas where Government could initially focus the regulatory reform agenda: (1) Governance and administration, (2) Reducing overlap and duplication, and (3) Standards and incentives.

First, on **governance and administration**, we consider there is a need to clarify roles and responsibilities for cyber security across the federal Government to ensure cyber security prevention and response is as effective and coordinated as possible, given the sheer number of agencies involved. This includes providing a clear statutory basis for the new National Coordinator and Office for Cyber Security, to empower it with the means to effectively coordinate the response to major cyber incidents across federal agencies, including appropriately sequencing and prioritising requests for information and reporting. The Coordinator and Office could also be empowered to undertake post-incident reviews that ensure we all heed lessons learnt from major cyber security incidents, similar to the Cyber Safety Review Board in the US. The clarification of roles and responsibilities across agencies needs to be accompanied by adequate resourcing for operational agencies to fulfil their functions, including for the Office of the Australian Information Commissioner.

Second, on **reducing overlap and duplication**, there are overlapping and duplicative disclosure and reporting requirements for data breaches across the federal government, as well as different levels of government, which hamper coordination efforts, slow down the disclosure process, and

[1] Home Affairs, 2021, *Strengthening Australia's cyber security regulations and incentives*

create unnecessary administrative burdens for companies that have experienced a cyber incident or data breach. Several agencies have similar, though not identical, information requirements and therefore separate reporting processes must be undertaken for each entity. Streamlining reporting and disclosure requirements should be a priority for the reform process to ensure we create a cyber security response environment that is responsive, agile and doesn't get bogged down in bureaucracy. This should include examining how to address the increasing reporting and disclosure requirements at a state and territory level, including exploring a potential referral of powers from the states and territories for cyber security and data breach matters to provide the federal Government with the capacity to institute a truly national approach.

We also support the recommendation in the Privacy Act Review to review laws across government requiring retention of personal information. Many of these laws have been in place for decades without review, raising questions about whether businesses are unnecessarily collecting sensitive personal information due to outdated legal requirements. The review could be accompanied by a new proactive review process for legislation proposing new requirements for data collection and retention of personal and sensitive information by government agencies or the private sector, to ensure proper scrutiny of new laws that could run counter to the Government's overall cyber and privacy policy objectives. This should include reviewing how the design of the program will take into account privacy and security considerations, and the governance and assurance program that will underpin its implementation.

Finally, on **standards and incentives**, Australian companies have expressed a need for clearer guidance on the cyber security measures they can and should take to mitigate and minimise risk. The Essential 8 provides this sort of guidance but is currently more focused on use of technology by the public sector and has a bias towards on-premises software solutions. While the principles behind the Essential 8 may be applied to cloud services and enterprise mobility, or other operating systems, they are practices appropriate to certain types of risk, but shouldn't be considered a substitute for comprehensive risk management. There are also a range of international standards that are highly relevant to the operations of Australian organisations, such as NIST's Cybersecurity Framework.

The Tech Council therefore supports updating the Essential 8, in line with equivalent international standards such as NIST's Cybersecurity Framework, to ensure it reflects current best practice and remains relevant to the economy at large. We also support the recommendation of the Privacy Act Review to clarify that "reasonable steps" under APP 11 would constitute both technical and organisational measures. This should be accompanied by clear and actionable guidance for organisations that could drive an uplift in positive cyber security behaviours. Given there is no clear single best practice standard, and in the interests of supporting interoperability and harmonisation, we encourage the Government to avoid a one-size-fits-all approach when incorporating standards in regulation or guidance – the approach taken to the SOCI Risk Management Program Rules is a good example of how to do this well. Further guidance tailored for small and medium-sized companies should also be provided.

We also support moving beyond rigid rule or penalty-based approaches to incentivise positive behavioural change. The Government has already introduced a new "big stick" with some of the highest penalties in the world for serious breaches of the Privacy Act. Given the sophisticated nature of many cyber attacks, we recommend balancing the "big stick" with models that provide organisations with an incentive to adopt best practice cyber security standards, support disclosure to relevant agencies (e.g. ACSC and OAIC), and encourage coordination/cooperation with authorities following a cyber incident or data breach. This should include exploring potential safe harbour models, building the cyber insurance market, SME certification processes, tax incentives and other mechanisms.

Government should also continue to prioritise legislation to enable the rollout of the trusted digital identity framework across the economy, which will support businesses to avoid holding 'honey-pots' of data and better protect customer privacy.

We encourage the Government to exercise caution on the proposal to add customer data and systems to the definition of critical assets under the Security of Critical Infrastructure legislation. The SOCI legislation is intended to apply a higher regulatory standard to a targeted list of facilities and assets that we rely on to underpin our society, businesses and lives and are critical to our national security, whereas customer data and systems are a common feature of almost all businesses in the modern economy. Adopting this proposal may run counter to a "risk-based" approach to cyber security regulation, be inconsistent with the definition of "critical infrastructure" and impose an unreasonably high regulatory standard on a large proportion of businesses across the economy (including SMEs).

As an alternative, we recommend the Government remain focused on prioritising rollout of the trusted digital identity framework to better protect customer data and privacy, and adopt the recommendations under the Privacy Act Review to clarify that "reasonable steps" under APP 11 would constitute both technical and organisational measures, and to enhance guidance on what "reasonable steps" are to secure personal information (including in relation to cyber security).

Recommendation 1: Focus the cyber security regulatory reform agenda on simplification, clarification and incentivising good behaviour. Reforms should be:

- Underpinned by an audit of existing laws and regulations to properly identify the key gaps, areas of overlap, duplication or conflicting requirements.
- Adopt overarching objectives and principles to ensure a coordinated and coherent reform agenda across areas such as cyber security, privacy, digital identity, electronic surveillance reform and online safety.

Recommendation 2: Initially focus regulatory modernisation efforts on:

- Governance and administration including:
  - Clarifying the roles and responsibilities for cyber security across federal and state Governments
  - Establishing a statutory basis for the new National Coordinator and Office for Cyber Security that empowers it to effectively coordinate the response to major cyber incidents across federal agencies and undertake reviews of major cyber security incidents that ensure we all heed lessons learnt and drive continual improvement
  - Ensuring operational agencies are provided with sufficient resourcing to fulfil their responsibilities, including the OAIC
- Reducing overlap and duplication including:
  - Streamlining overlapping and duplicative disclosure and reporting requirements for cyber security incidents and data breaches across the federal government to make cyber incident response agile, responsive and ensure it doesn't get bogged down in bureaucracy
  - Examining how to address overlapping reporting and disclosure requirements at the state and territory level, including exploring a potential referral of powers that would enable the federal Government to institute a truly national response

- Supporting the recommendation in the Privacy Act Review to review laws across government requiring retention of personal information
- Stablishing a proactive review process for legislation proposing new requirements for data collection and retention of personal and sensitive information by government agencies or the private sector, to ensure proper scrutiny of new laws that may run counter to the Government's cyber and privacy objectives

- Standards and incentives including:
  - Improving existing standards and guidance, including updating the Essential 8 in line with equivalent international standards, and supporting the recommendations of the Privacy Act Review to clarify that "reasonable steps" under APP 11 would constitute both technical and organisational measures, with enhanced accompany guidance from the OAIC – to help drive cyber uplift across the economy
  - Examining models to provide organisations with an incentive to adopt best practice cyber security standards, support disclosure to relevant agencies (e.g. ACSC and OAIC), and encourage coordination/cooperation with authorities following a cyber incident or data breach (which may include exploring potential safe harbours, building the cyber insurance market, SME certification processes, tax incentives and other mechanisms)
  - Continue to prioritise legislation to enable the rollout of the trusted digital economy framework across the economy to support businesses avoiding holding 'honey pots' of data and better protect consumer privacy
  - Create regulatory frameworks that enable businesses to safely, securely and legitimately share customer data following a data breach, in the interests of preventing further harm.

Recommendation 3: Do not support the proposal to add customer data and systems to the definition of critical assets under the SOCI legislation.

3.1.2 Secure-by-design and -default for technology providers

The Tech Council recognises that there are shared responsibilities for cyber security across the supply chain. This includes technology and software providers, but it also includes users of technology (organisations and individuals) and the processes they put in place.

People, processes and technology are known as the three pillars of cyber security, and we caution governments against over-emphasising the capacity of one part of the supply chain to act as a silver bullet. Data on the causes of cyber security incidents and data breaches demonstrates that breaches related to software systems are amongst the least likely reasons for a breach:

- 82% of breaches globally involve the human element – including social attacks, errors and misuse[2]
- 70% of domestic breaches reported to the OAIC are from malicious or criminal attack, 25% from human error and 5% from system fault, and of those caused by cyber security incidents, around 60% are due to compromised or stolen credentials[3]

[2] Verizon 2022, Data Breach Investigations Report
[3] OAIC 2022, Notifiable Data Breaches Report: July to December 2022

- Placing more responsibility or liability on software providers won't address these people and process issues, nor would it have necessarily prevented recent large-scale breaches in Australia. Examples of how people are exploited as a vulnerability include phishing attacks, scams and utilising personal devices without enterprise security features. Processes within organisations can also create vulnerabilities, such as the way other applications are integrated into software, or relying on old or outdated legacy systems (the health and medical sector is a good example here, and is also consistently the number one sector for data breach notifications).

The shared roles and responsibilities of different players in the supply chain differ depending on the type of software provided. For example, Software-as-a-Service products deployed on cloud infrastructure involve the software developer managing updates, patching and all the physical, infrastructure and network security related to that application. However, the end user may still be responsible for security relating to access, passwords, identity management and authentication, as well as the integration of the SaaS product with other applications. On the other hand, for on-premises software (commonly used in government agencies and in many other parts of the economy), while the software developer remains responsible for ensuring the software is developed securely and that potential vulnerabilities are identified and managed, it is the end users who are responsible for ensuring that the software is upgraded and that security patches from the developer are deployed. The end user is also responsible for physical, infrastructure, network security and integration of other systems.

This is not to say that there isn't a critical role for technology and software providers. We recognise that there is significant scope to improve secure software development standards and guidance, which remains a relatively nascent area in Australia and internationally. We encourage the Government to take an approach here that prioritises international interoperability and harmonisation, particularly given most technology products sold in Australia are not produced here (while we have a globally successful and growing sector, Australia's direct tech sector remains much smaller than many other countries, including the US, UK and Canada).

With this in mind, we welcome the ACSC's participation in the recently released co-sponsored guidance on *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and-Default*. The multilateral approach adopted here, with the involvement of US, Australian and European agencies, is a helpful development, and we encourage continued engagement by the Australian Government in these processes, alongside a more concerted effort to engage with Australia's tech industry (which has not been involved to date).

We understand the Government and expert panel are now considering whether secure-by-design and -default requirements could be embedded in the Australian regulatory framework. Given this is a nascent area of regulation, there needs to be more fulsome consultation and engagement with industry on this, taking into account the following matters:

- Secure software development standards are still relatively immature, and lack the necessary infrastructure (e.g. measurement, certification, auditing infrastructure) required that would allow for meaningful regulation at the present time. We note that in the US, the NIST Secure Software Development Framework, which was only released in 2021, is largely implemented via government procurement and contracting with companies attesting that their products meet the framework;
- Australian tech companies and the Australian Government have not been meaningfully involved in the development of international secure software development standards to date – meaningful industry engagement is essential in standards development (particularly for those involving regulation) to ensure technical feasibility and effective implementation;

- There needs to be recognition of the shared responsibilities for cyber security and an understanding in government agencies that it is not possible to simply "engineer" out cyber security vulnerabilities (as threats and malicious actors continue to evolve alongside security improvements) and absolve users/customers of any responsibility;
- Regulatory proposals should involve proper cost-benefit and regulation impact analysis, including considering the level of impact such proposals would have had in preventing recent major cyber incidents and data breaches in Australia; and
- Any future regulatory models should be risk-based and focused on incentivising uptake of standards within software companies (e.g. through safe harbour frameworks). Punitive measures or liabilities would create substantial litigation and red tape for software firms (which would be felt most by smaller firms) and impact the Government's goal of growing our tech sector and reaching 1.2 million tech jobs by 2030, potentially for little cyber security gain.

Recommendation 4: The new cyber security strategy should reflect the shared responsibilities for cyber security across the supply chain, including the important and distinct roles of people, processes and technology.

Recommendation 5: The Australian Government should continue to engage in international processes on secure-by-design and -default guidance for technology providers, including the development of relevant standards, to ensure Australia takes an approach that is interoperable and harmonised. It should also establish a process to meaningfully engage the Australian tech sector in these processes.

Recommendation 6: We do not support any immediate moves by Australia to regulate secure-by-design and -default requirements or mandate secure software development standards, given they remain relatively immature and lack the necessary standards infrastructure at the present time, but would welcome an opportunity to engage with the Government on alternative models to drive engagement and uptake of these standards in the Australian tech sector, and to participate in cost-benefit and regulation impact analysis processes for any future regulatory proposals.

3.2. Strengthening International Strategy

As mentioned in the previous section, Australia, as a relatively small player in the global technology market, should be more engaged with international standards setting processes (such as ISO) to ensure that our technology and cybersecurity practices are up to par. Given that Australian tech companies operate globally and are often subject to international standards and requirements, it is essential that we create an aligned regulatory landscape that adheres to international best practices and standards to ensure the competitiveness of our home-grown talent. We can also seek to leverage the work that is currently undertaken in allied markets such as the United States through the National Institute of Standards and Technology (NIST).

The Tech Council also support an outcomes and principles-focused approach to international standards which is critical in a rapidly evolving cybersecurity landscape, where best practices do evolve quickly. This ensures a focus on desired behaviours and outcomes, rather than prescriptive rules and regulations that may be quickly obsolete. This promotes regulatory agility and flexibility, to also enable the adoption of new technologies and regulatory practices as they emerge.

Recommendation 7: The Australian Government, working with industry, should enhance its engagement in international standards setting processes for cyber security, and better leverage and align our standards with work being done in allied markets such as the US NIST.

3.3. Securing Government Systems

The criticality of cybersecurity in national security is uncontested. Government agencies have a significant responsibility to ensure the protection of sensitive information, processes, and for the benefit of our consumers and citizens. As such, it is imperative that senior leaders in government, across all agencies and departments are held to the same standard of accountability as industry CEOs on cyber issues and incidents. This is necessary to enforce guidelines and measures to safeguard and protect against potential cyber threats. By implementing an accountability framework for senior government leaders, we can ensure that we remain proactive and vigilant in maintaining the security of our national systems and data.

In addition to senior accountability, government could benefit from increased use of industry standards and best practices in cyber. The development and adoption of technology systems and platforms used within government should adhere to frequent patching and updates, best practice development processes, as well as regular product release cycles. The cybersecurity strategy can also consider how to leverage industry expertise and technologies through public-private partnerships to secure government systems, which is discussed further in Section 4.1 below ('Improving public-private mechanisms').

Recommendation 8: Government should introduce a cyber security accountability framework for the Australian Public Service that holds agency and department heads to the same standards as industry CEOs and Directors.

4. Response to Areas for Potential Action

4.1. Improving public-private mechanisms for cyber threat sharing and blocking

The Government's Cyber Security Industry Advisory Panel has previously noted that "threat sharing is the key to identifying malicious activity, which is the key to threat blocking". However, the current ACSC mechanisms to enable sharing of threat intelligence are not working as effectively as intended.

To improve threat sharing and blocking requires Government to be more open with intelligence and less 'black box' which involves sharing information back to the industry/security community to improve intelligence flows both ways, rather than take an extractive approach to the information provided by industry. Given that government and industry hold different information and see different threat vectors, sharing information would enable both parties to understand the gaps and to work together. This would include sharing, for example, the unique 'fingerprints' of malicious actors with industry to support more effective threat blocking.

More importantly, the foundations for effective mechanisms in cyber threat sharing and blocking demands a bigger shift in government and how it approaches its relationship with industry. This involves the government adopting an approach that moves beyond reporting and 'check-the-box' engagement with industry, or a 'big stick' approach that results in increased penalties and liabilities. We have an opportunity now to move towards a more sophisticated model of public-private partnerships. This is especially important given the increased number and sophistication of cyber security attacks and data breach incidents which inherently demands improved mechanisms of coordination and collaboration.

By fostering genuine collaboration and trust between industry and government, this would enable industry to better aid and assist government in meeting cybersecurity goals and outcomes in the common national interest. We can rise to meet the shared responsibility and challenge that comes with tackling cybersecurity from a true united front. Underscoring all of this is the

promotion of a culture of shared responsibility between government and industry which creates an effective and cohesive whole of nation cyber security strategy which the government now seeks to create.

The benefit of doing this means that we can bring together experts from both public and private sectors who can share knowledge, skills and resources to better understand and respond to cyber threats, identify emerging threats and vulnerabilities, as well as improve our overall cyber security posture as a nation.

One example of where this could be enhanced is through the establishment of industry testing labs under the Government's "Secure G" initiative, which brings together government, industry and academia and help organisations test protocols, measures, standards and software to support the deployment and secure implementation of 5G. There is an opportunity to adapt this model to allow critical sectors to test end-to-end security of their applications prior to deployment at scale, ensuring any vulnerabilities can be properly identified and addressed.

We also recommend that the ACSC be reaffirmed as the central point of contact for cybersecurity incidents amongst industry, consumers and government. As such, the ACSC's role can be evolved to be more open and cooperative to build trust in the security community with these suggestions below:

- The model for community could be improved by, drawing on best practices overseas which operate at a national level and have a more regular cadence of meetings (e.g. FBI and FS-ISAC models).
- There is an opportunity to create industry-specific threat sharing communities (e.g. mining, banking, tech) within the existing structure of the ACSC, which could be run by self-governed committees.
- The ACSC could invite individuals to the intel sharing community on a person-by-person basis, instead of company. Individuals would be more comfortable sharing more detail if it was clear who was present and attendees were operating under a signed NDA.
- The ACSC should improve on community governance by considering appropriate boundaries/protocols for vendors participating in existing intel sharing communities to help establish trust and legitimate intelligence sharing.

There is significant room and opportunity when industry and government work together in a genuine collaborative partnership, together in the form of a national integrated public-private taskforce which can help assist with joint cyber operations and cyber activities. This could include for example, joint threat hunting teams and coordinated cyber exercises where multiple teams and organisations work to identify and mitigate cyber risks and threats by leveraging the resources and expertise of all participating entities. These opportunities also provide a chance for collaboration and knowledge-sharing amongst different parts of our national cyber workforce to better enhance our overall cybersecurity resilience, as a nation.

Recommendation 9: Government to reframe its approach to collaboration with industry by taking a more open, two-way approach to sharing of information and intelligence to better enhance cyber threat sharing and blocking.

Recommendation 10: Adopt an approach to creating sophisticated public-private partnerships which foster genuine trust, one that enables industry to aid government in meeting our common cybersecurity goals as a nation.

Recommendation 11: Consider enhancing the "Secure G" testing labs initiative to allow critical sectors to test end-to-end security of their applications prior to deployment at scale.

Recommendation 12: Improve threat sharing by increasing the cadence of threat sharing meetings, create industry and practice specific threat sharing communities, curate the intel sharing community based on expertise and company role, and consider appropriate boundaries and protocols for vendors in intel sharing communities.

4.2. Supporting cybersecurity workforce and skills pipeline

Australia has major skills gaps in its technology and cyber security workforce. Our research shows that vacancy rates in tech roles are 60% higher than the national average, while the vacancy rate for cyber roles is more than double the national average. These include specialist technical and experienced roles like cyber security specialists, as well as other roles that directly affect our cyber capabilities, such as software engineers and network architects.

These shortages weaken our cyber security environment by starving tech companies and other businesses across the economy from the skills they need to develop quality products and services. This includes impacting the capacity of software firms to adhere to secure software development best practices.

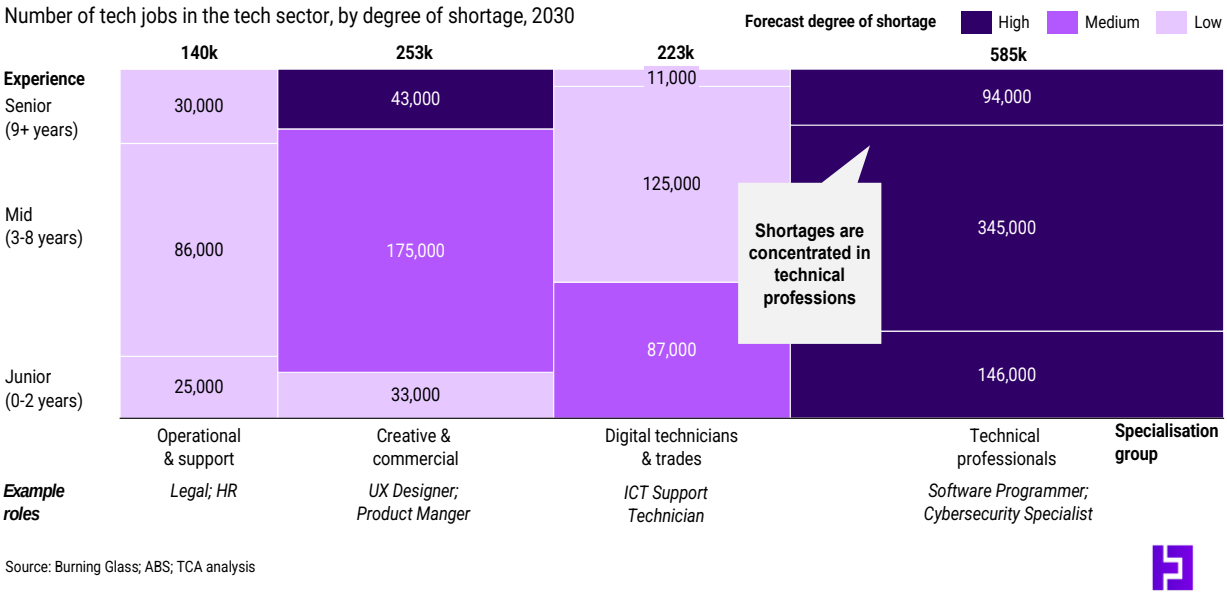
The new national cybersecurity strategy needs to consider innovative and forward-thinking ways to build our cyber workforce pipeline. The demand for tech jobs strongly outweighs the supply of labour that we have available in Australia and if not addressed now, will be exacerbated by 2030.

The TCA recommends prioritising action in this area, which will serve to bolster cyber security within Government and across the economy.

4.2.1 Skilled Migration

Skilled migration plays a crucial role in filling tech and cyber security roles. Just over a third of forecast tech vacancies by 2030 are in highly technical roles requiring 3+ years' experience (figure 1). These roles cannot be quickly filled by the local workforce given the long lead times for training and low skills match – only 7% of the non-tech workforce have similar skills, limiting the opportunities for rapid retraining. We will need around 439,000 people in technical roles requiring 3+ years' experience by 2030.

Figure 1: Demand for tech jobs by 2030 by experience and specialisation



Source: Burning Glass; ABS; TCA analysis

We welcome the Government's decision to review the skilled migration system and have been engaging closely in that process.

The inefficient administration of Australia's migration system has long constrained our ability to attract experienced tech workers. While we welcome the Government's investments to clear the visa backlog and welcome the fact that processing times have substantially improved, the average time to process short-term skilled visas is still 2-3 times longer than competitor countries like Israel and Canada, which have expedited paths for tech workers. Improving visa processing times would provide an immediate pressure-relief to support Australian tech companies to attract global talent and build capability within entry level and mid-level domestic technical talent.

To maximise the economic benefits from skilled migration we make three recommendations in our submission to the review of the migration system:

- Prioritise employer-sponsored skilled migration, with fast pathways to permanency and increased labour mobility.
- Streamline arrangements for visa holders earning above a defined salary threshold for accredited sponsoring employers, by removing occupational specification, labour market testing and skills assessments.
- Ensure the administration of the skilled migration program is internationally competitive, including by committing to a visa processing service standard of 10 days (on average), modernising the accreditation pathways for sponsoring employers, and better targeting the use of SAF levy funds.

There are also further steps the Government could take in the shorter term. Of the 12 tech roles facing the most acute and ongoing shortages in the tech sector, just three — business analysts, network professionals (network engineers) and software programmers — are on Australia's Medium and Long-term Strategic Skills List that enable permanent residency. This is an area for review, and we encourage the government to review the Strategic Skills List to ensure that all related tech and cyber security professions are captured. In addition, we can also work to remove age limitations on permanent visas such as the 186 which prevents experienced cyber specialists coming to Australia.

Our world-class universities also attract hundreds of thousands of international students each year, yet only 28 per cent use their post-study work rights and just 16 per cent become permanent residents. The recent extension of post study work rights for international students will be an important element of improving Australia's ability to leverage graduate capability, we can work further to simplify the pathway to permanent residency for international student graduates in tech fields to retain capability. Additionally, we could enable all international students in skills shortage roles to automatically be awarded a 485 visa upon successful completion of their qualification without having to submit an application. This could be complemented by government working with industry to change the perception of the difficulty of employing international students to increase retention rates of trained graduates.

Recommendation 13: The Government's response to the review of the migration system should seek to:

- Prioritise employer-sponsored skilled migration, with fast pathways to permanency and increased labour mobility.
- Streamline arrangements for visa holders earning above a defined salary threshold for accredited sponsoring employers.

- Ensure the administration of the skilled migration program is internationally competitive, including by committing to a visa processing service standard of 10 days (on average).

Recommendation 14: Review the Strategic Skills List to ensure that all relevant cyber-security professions are captured and remove age limitations on permanent visas such as the 186, which prevents experienced cyber specialists coming to Australia.

Recommendation 15: Simplify the pathway to permanent residency for international student graduates; enable all international students qualified in skills shortage listed roles to be automatically awarded a 485 visa upon completion, and work with industry to change perceptions around the difficulty of employing international standards to increase retention of trained graduates.

4.2.2 Education and training

At present, Australian qualifications for cyber are not fit-for-purpose and are negatively contributing to the workforce shortage as graduates are not job-ready to enter the workforce. The rapidly changing nature of technology and the threat landscape means that cybersecurity is constantly evolving, and it is essential that students are trained on the latest tools and techniques faced by industry. The curriculum of existing qualifications lacks practical, hands-on experience that is necessary for success outside the classroom and many graduates have a limited understanding of how to apply their knowledge in real world-scenarios. Part of the solution here could be piloting cyber security as a test case for a Skills Standard and testing framework (rather than relying on the existing qualifications-based system) which can better recognise and integrate high-quality industry training content.

New and improved pathways into cyber and innovative training opportunities will also ensure that skills developed are relevant and up to date, providing a strong starting point for those who are interested in, or transitioning into, cybersecurity. We strongly support the Digital and Tech Skills Compact announced at the Jobs and Skills Summit, including the development of a Digital Apprenticeships model. We recommend that a cyber security stream to be included in the design of the program which will help build the talent pipeline for the future.

There is also an opportunity to address knowledge and awareness of cybersecurity careers earlier in the student journey. Cyber could be holistically embedded throughout the education system from K-12 and into tertiary education courses (e.g. cyber can be considered a teachable 'risk' in business schools/courses, for example). This can help support overall long-term cultural change in nurturing home-grown talent, cyber awareness, and cyber resilience. The Tech Council is also working to establish a virtual work experience program for tech jobs that would be accessible to secondary school students, and which could include a cybersecurity stream.

Finally, the Government could consider additional Commonwealth supported places for cyber security related qualifications as well as wage subsidies to encourage more businesses to take on cyber trainees and apprenticeships, or work with industry to commit to a quota of tech internships and graduate placement positions.

Recommendation 16: Embed cyber education modules and units from K-12 and into tertiary education courses (e.g. including cyber as a teachable 'risk' in business schools/courses) to support long term-cultural change in cyber resilience.

Recommendation 17: Review the existing education and training curricula for cyber-related VET and higher education qualifications, and pilot cyber security as a test case for a Skills Standard and testing framework which can better recognise and integrate high-quality industry training content.

Recommendation 18: Continue to support the work of the Digital Skills and Training Compact Working Group to design and deliver a modern digital apprenticeship model with a specific cyber-stream to assist new entrants and individuals seeking to transition into cyber (and consider wage subsidies to drive uptake).

Recommendation 19: Provide additional Commonwealth supported places (CSPs) for cyber related qualifications.

4.2.3 Diversity, perception, and awareness of cyber careers

Further effort is needed to normalise and communicate the diversity of roles, backgrounds, skills involved in cybersecurity. For example, women make up only a quarter of Australia's tech workforce[4], and it's estimated that this is even lower in cyber security. This is despite tech jobs being amongst the most well-paid, fastest-growing, secure and flexible jobs in the economy, with half the gender pay gap of other high paying industries. Supporting more women to skill and reskill into tech and cyber roles should be a priority for both addressing workforce shortages and supporting women's economic security. The current review of women in STEM / diversity programs should include research on the barriers and opportunities to support more women into tech and cyber roles.

One of the barriers to getting more Australians from more diverse backgrounds to enter the tech and cyber workforce is the lack of awareness of the career opportunities. This is occurring at all levels of workforce engagement, and partly contributes to the poor levels of diversity in tech and cyber jobs. A heightened awareness of cyber careers across all age-groups increases the chance of individuals selecting these roles as a viable career option, attracting individuals from diverse backgrounds and unlocks a greater number of possible workers.

Demystifying cybersecurity roles can highlight that there are many different roles, both technical and non-technical (i.e. risk management, compliance) that individuals and graduates can uptake. The cyber strategy could pursue improvements to professional mentoring, networking, and development programs aimed at university students. It could also coordinate engagement with tertiary stakeholders and student associations and societies to demystify graduate opportunities in cybersecurity.

Recommendation 20: Leverage the current Diversity in STEM review to focus on identifying barriers and opportunities to support more people from diverse backgrounds into cyber roles.

Recommendation 21: Government and industry to coordinate engagement with tertiary stakeholders and student associations to demystify graduate opportunities in cybersecurity, including by supporting professional mentoring, networking and development programs.

4.3. National framework to respond to major cyber incidents

Recent major cyber security incidents and data breaches have demonstrated the need for a more structured and coordinated national response framework, particularly to improve coordination across federal government agencies, different levels of government, and with relevant industry players.

A more formal and coordinated national response and review framework could enable better sharing of information, leveraging of resources, improved support for affected individuals, and enable a cycle of continual improvement in industry based on lessons learnt. This will ultimately build a more effective and resilient cyber security landscape.

[4] Tech Council of Australia and Accenture, 2022, *Australia's Tech Jobs Opportunity*

As mentioned above, the current models for preventing and disclosing cyber-incidents also need to be reviewed and enhanced given the intensifying threat environment and emerging evidence of policy gaps and issues. Following a cyber-incident, there is an overwhelming volume of reporting and investigation requirements which can often put unnecessary pressure on an organisation's immediate operational response, which should be more appropriately focused, on understanding and minimising the impact of the cyber incident.

The new National Coordinator and Office for Cyber Security – if underpinned with the appropriate statutory powers – could ensure the response across government is better coordinated, sequenced and prioritised (including ensuring there is a phased approach and timelines to 1) operational response; 2) enforcement; and 3) regulatory reporting). It could also institute a more formal review process for major cyber incidents, taking account of lessons learnt from international models such as the US Cyber Safety Review Board and similar domestic models such as CASA's airline safety incident reports. We also encourage efforts to streamline and reduce duplication of reporting and disclosure obligations, to lessen the burden on organisations who have experienced a cyber incident, enabling them to better focus their efforts on immediate operational response.

Our national response capabilities could also be potentially enhanced by expanding military reserve positions for cyber security in the Australian Defence Force. This would enable leading Australian talent to contribute to the national cybersecurity effort without sacrificing their established private industry careers.

Finally, we would encourage the Government, through the Australian Communications and Media Authority, to consider the role and standards for the media in reporting on cyberattacks. Cyber incidents can be complex, and it can be challenging to accurately determine and report on the details of an attack. Inaccurate or incomplete media reporting can at best lead to confusion and misinformation, and at worst, disclose sensitive information that could compromise ongoing investigations and jeopardise the efforts of law enforcement and other agencies. We recommend developing guidelines for reporting on cyber incidents. This is already done for other sensitive areas, such as suicide reporting.

Recommendation 22: Institute a more formal and structured national response and review framework for major cyber security incidents, which could be led by the new National Coordinator and Office for Cyber Security.

Recommendation 23: Expand military reserve positions for cybersecurity in the Australian Defence Force to increase our national response capabilities.

Recommendation 24: Consider the appropriate role of the media in reporting on cyberattacks through the Australian Communications and Media Authority and develop guidelines for reporting on cyber incidents (similar to what is done for other sensitive areas, such as suicide reporting).

4.4. Community awareness and victim support

Cybersecurity risks continue to evolve, and new threats continue to emerge. Ongoing education and awareness-raising initiatives are necessary to ensure that individuals and organisations in Australia remain vigilant, with the appropriate knowledge and skills, to protect themselves against cyber threats.

One approach is through an improved national educational and awareness campaign. Such a campaign would focus on promoting simple best practices and behaviours for cybersecurity amongst individuals, which could take account of the success of the 'slip, slop, slap' campaign for sun safety. In addition to general public awareness and education, consideration should also be provided on how to target senior Australians, vulnerable individuals, and those with language

barriers who may be particularly vulnerable to cyber threats - such as identity theft, online scams and fraud. As they may be less familiar with technology and have limited understanding of the risks associated with it, these groups are far more represented in those suffering loss compared to others and the Government could consider targeted campaigns for these demographics.

We also suggest that there is a bigger role for the ACSC to play in the broader community which includes greater awareness, education, basic cyber skills training, as well as providing baseline support to organisations, individuals, and consumers who have experienced cyber incidents.

The cyber security strategy can also assist in uplifting cyber awareness and readiness amongst small and medium sized enterprises. A significant proportion of our economy is made up of small businesses, which has significantly less resources, capability and knowledge to dedicate to cyber security. In bolstering the role of the ACSC, we can also take inspiration from the United Kingdom, which has established 'Resilience Centres' that support small and medium sized organisations and enterprises by providing cyber and ICT support through industry partnerships. This could be further enhanced by considering how to encourage larger businesses and government agencies to apply cyber standards and certification requirements for SMEs through their supply chains. We note that there are already independent industry-maintained certification schemes designed for SMEs that are being rolled out that could be leveraged. The Government should also consider the outcomes of COSBOA's pilot Cyber Security Wardens program to determine options for expansion.

Another mechanism to achieve small business uplift is through the Technology Investment Boost and Skills and Training Boost tax incentive measures for small businesses which can be allocated to cyber security uplift and training. The Technology Investment Boost provides small businesses with a 120% tax deduction for investments in digital adoption, while the Skills and training Boost provides the same deduction for investments in skills and training. The Government could work with industry to better communicate the way these tax incentives can be used by SMEs to get a cyber audit, enhance adoption of security technologies and train staff.

Recommendation 25: Implement a national cybersecurity education and awareness campaign ('slip, slop, slap') to promote best practices and behaviours to increase overall cyber awareness across the nation.

Recommendation 26: Elevate the role of the ACSC and increase resourcing to better support the community through basic skills training, support to organisations and individuals who have experienced cyber incidents.

Recommendation 27: Uplift cyber readiness amongst SMEs by encouraging industry/government to consider cyber standards and certification requirements across procurement and supply chains, and consider the outcomes of COSBOA's pilot Cyber Security Wardens program to consider options for expansion.

Recommendation 28: Leverage the Skills and Training Boost, as well as the Technology Investment Boost as tax measures to incentivise SMEs to uplift their cybersecurity processes, technologies and practices.

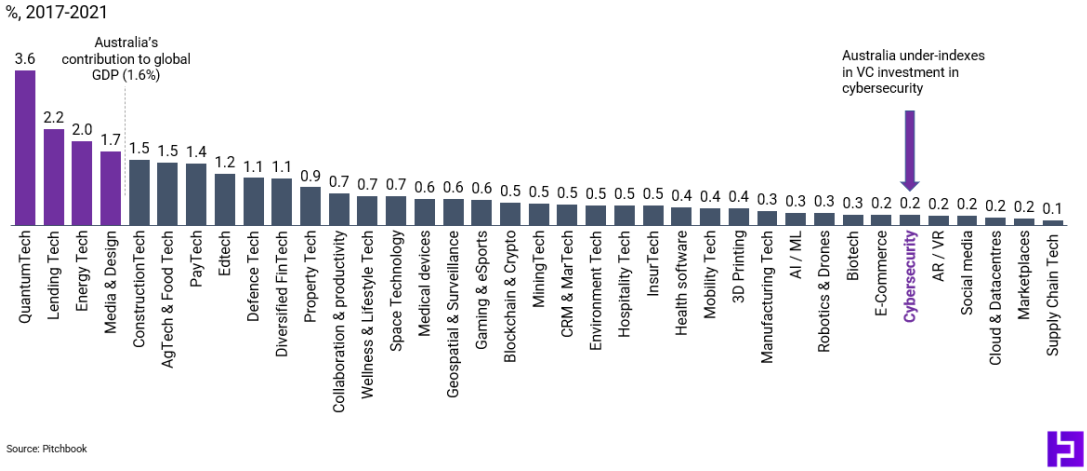
4.5. Investing in the cyber security ecosystem

While Australia has a vibrant ecosystem for cyber security start-ups and scale-ups, we significantly under-index on investment in our cyber industry compared to other countries.

While we have a 1.8% share of global cyber security start-ups, we only attract a 0.24% share of global venture capital investment into these businesses, which is significantly lower than our 1.6% share of the global economy and the share of venture capital attracted by other Australian

tech segments[5] (see **figure 2**). This is consistent with an overall under-investment in other critical technology areas such as AI, robotics and biotech. Cyber security startups not only need to demonstrate a return on investment, they also need to have sufficient up-front capital to establish a minimum viable operation that can scale effectively. Moreover, AustCyber's latest Cyber Security Sector Competitiveness Plan also shows that our cyber sector's revenue growth falls behind leading nations and only 50% of our cyber companies are exporting, despite Australia having a relatively small domestic market[6].

Figure 2. VC funding in Australia as a share of Global VC funding by market segment



The strategy should consider how the Government can address this funding gap and help co-invest in the cyber industry by leveraging existing initiatives such as the $15 billion National Reconstruction Fund. Enabling technologies are one of the 7 priority areas for investment under the NRF equity and loan facility, providing an opportunity to address this market failure.

Cyber security start-ups, similar to many other segments of the tech sector, also rely heavily on securing foreign venture capital, highlighting the importance of creating more efficient foreign investment review processes. Currently, Australia has the 34th least efficient foreign investment review process amongst 38 OECD countries.[7] That places Australia behind allies like the US and UK, and countries such as Turkey, Poland and Chile. This is a major issue for the tech sector, with around two thirds of all tech deals involving some level of foreign direct investment. Foreign investment is a valuable source of funding and streamlining administration of the FIRB process can reduce the administrative burden and time required for investors to pool funds into Australian cyber startups.

Finally, the strategy could encourage Government to develop the cyber security start-up ecosystem by engaging at very early stages with these businesses either as collaborators or early-stage clients. This approach helps start-ups refine their solutions and develop products that meets the specific needs and requirements of government agencies, as well as other potential customers. Input on regulatory compliance, risk, management and other key factors can be incredibly valuable for early-stage startups. These are essential requirements for start-ups to grow to a stage of viability as we see in other countries like Israel that is now leading the world in this area.

[5] Tech Council of Australia and McKinsey, 2022, *Turning Australia into a Regional Tech Hub*
[6] AustCyber, 2022, *Australia's Cyber Security Sector Competitiveness Plan 2022*
[7] OECD, 2020, FDI Regulatory Restrictiveness Index

Recommendation 29: Address funding gaps and market failures in venture capital investment for Australian cyber security firms through existing funding mechanisms, including the National Reconstruction Fund.

Recommendation 30: Streamline and improve administration of the foreign investment review process to remove barriers to foreign investment in cyber-startups.

Recommendation 31: Government to engage with early-stage cyber-security startups by providing early input as a customer, to help refine product and user requirements, and input on regulatory compliance to assist in scaling (reflecting the challenges Australian firms face in attracting sufficient funding to scale and remain onshore).

4.f. Designing and sustaining security in new technologies

The Tech Council is encouraged to see consideration of new technologies in the 2023-2030 Cybersecurity Discussion Paper. The technological landscape is constantly evolving, rapidly changing, and new and emerging technologies will present both opportunities as well as challenges to the cybersecurity landscape. Currently, Australia does not make full use of existing technologies that can strengthen cyber security and there is room for improvement. This includes:

1. Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA). 2FA and MFA are examples of an available and accessible technology practice that can significantly enhance cyber security for individuals and businesses, but which largely remains voluntary across most services. The updated cyber security strategy should consider the Government's position on strongly encouraging, or in higher-risk scenarios potentially mandating, these technologies and/or standards.
2. Data encryption. The new cyber strategy should set a clearer whole-of-government direction on the benefits of encouraging or mandating the encryption of stored sensitive data by enterprises to minimise cyber security risk across the Australian economy. The debate in recent years about the potential downsides of encryption (e.g. enabling criminal activity and reducing access to information for law enforcement) has sent mixed signals to businesses about the appropriateness of encrypted data.
3. Decentralised Data Storage. The new cyber strategy should consider the increased use and uptake of decentralised data storage models and consider mechanisms to achieve this (the NSW Government's digital identity system provides a good example of the practical application of decentralised data storage). To increase security for data storage, decentralised data is encrypted and stored across multiple locations, or nodes. In this setup, only the data's owner holds a private encryption key. Decentralised storage also delivers benefits such as data immutability, enhanced privacy and overall security by ensuring that data storage does not have a single point of failure.
4. Data Classification, Loss Prevention and Decommissioning: Many companies do not know the extent of the sensitive data that they hold across their business, and therefore do not know the extent of the risk they face. This can be mitigated through Data Classification and Data Loss Prevention technologies, which can help stop employee or customers details (and other sensitive information like IP or financial data) from being sent, either accidentally or intentionally, outside the corporate network. Moreover, the government could also provide guidance for data deletion and decommissioning practices and procedures which would assist organisations to dispose of sensitive data that is not needed to minimise the 'blast radius' and severity of attacks.
5. Expansion of the trusted digital identity framework. Digital identity and digital credentials systems enable consumers to establish a digital ID once and use it repeatedly to prove their

identity for a range of online services. This saves businesses and consumers time and money, while avoiding the need for organisations to collect and store sensitive information. The NSW Government's decentralised digital identity model is illustrative of how new technology can support greater privacy and citizen control over their identity. This is also acknowledging that legislation is required to support the rollout of the federal Government's trusted digital identity framework accreditation model across the states and territories and the private sector. Accelerating the rollout could significantly decrease the business-as-usual risk posed by organisations holding personally identifiable information within their own systems.

In addition to adoption of existing technologies that enhance cybersecurity, Australia must look to investing in emerging technologies of to safeguard resilience for the future. This includes competitive investment in research and the commercialisation of technologies across IoT, AI and quantum. As cybersecurity threats continue to become more advanced and sophisticated, the combination of these technologies will significantly advance the scale and speed in which cyber incidents occur.

6. Internet of Things: IoT devices are pervasive and ubiquitous in our daily lives, from smart homes to smart infrastructure, and smart cities. The security of these devices is, however, often neglected. One of the main challenges at present of securing IoT devices is that they are often designed with limited processing power and memory, which makes it difficult to implement robust security measures. Given their connection to networks with other devices, they also create a potential vulnerability as an entry point for attackers.
7. Artificial intelligence: The boon of generative AI and large language models just this year has seen the accelerated adoption of AI technologies in the mainstream. For cybersecurity, AI can be used by malicious actors to launch more sophisticated and targeted attacks. AI-powered malware for instance, may learn and adapt its algorithms to avoid detection by modifying its code to bypass traditional security measures. In phishing scenarios, AI powered chatbots or voice assistants can also be used to automate these types of attacks to impersonate a trusted entity or individual. Inversely, AI could also be used to enhance cybersecurity to automate threat detection and response. For example, ML algorithms can analyse large volumes of data and reveal patterns that may be indicative of a cyber-attack, or improve authentication methods by analysing user behaviour and identify anomalies that may indicate unauthorised access.
8. Quantum computing: The advent of quantum computers is expected to revolutionise computing. Quantum computers use quantum bits, or qubits, which can exist in multiple states simultaneously, making them exponentially more powerful than the processing that is done by classical computers. This also makes quantum computing capable of breaking many of the encryption methods used to secure data in the present day. This, combined with the fact that it is widely accepted that adversarial nation-states are building quantum computers to deploy maliciously. We need to start to consider post-quantum cryptography and quantum resilient requirements, starting with sensitive government data sets (similar to US National Security Memorandum No. 10, H.R.7535, the Quantum Computing Cybersecurity Preparedness Act).

Investing in innovative technologies for cybersecurity is not just an option, but a necessity to securely safeguard and protect Australia.

Recommendation 32: Promote technology innovation and adoption and consider how to prepare for emerging risks over the period up to 2030. This includes the adoption of 2FA/MFA, data encryption, decentralised data storage, as well as data classification and data loss prevention technologies and practices.

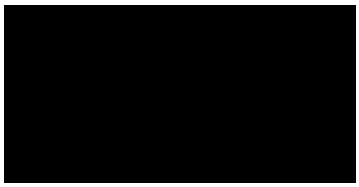
Recommendation 33: Continue competitive investment into research and the commercialisation of new and emerging technologies, this includes retaining existing and increasing funding for quantum technologies, IoT, and artificial intelligence.

Recommendation 34: Expand the trusted digital identity framework across the states and territories to reduce the need for organisations to hold personally sensitive information.

Recommendation 35: Consider quantum-resilient requirements including developing a plan for post-quantum cryptography, starting with sensitive government datasets.

We appreciate the opportunity to provide feedback on the 2023-2030 Cyber Security Strategy. We would be happy to continue this dialogue with the Expert Panel and the Department of Home Affairs to discuss our submission in further detail and help support the adoption of these recommendations.

Yours Sincerely,



Kate Pounder
CEO, Tech Council of Australia

[redacted]