Together we ideate. innovate. impact.

27 January 2023

Budget Policy Division
Treasury
Email: PreBudgetSubmissions@treasury.gov.au

re: Stone & Chalk Group 2023-24 Pre-Budget Submission

Thank you for providing us with an opportunity to comment on the Australian Government's consultation for the 2023-24 Federal Budget, led by the Treasury.

About Stone & Chalk Group
As the largest innovation community in Australia, our mission at the Stone & Chalk Group is to transform Australia into a sustainable tech-driven economy.

There are opportunities presented by emerging technologies and it will be important to ensure that we have a sustainable local technology industry in Australia. With a strong innovation ecosystem, this will in turn lead to more job opportunities and enable Australian businesses to become more globally competitive in the long term. This can be realistically achieved if we have an entrepreneurial pathway for accelerators and a more curated innovation ecosystem.

To support this, we need to have access to a sustainable pipeline of talent and skills to meet the demands of the emerging high-tech industries. We also need to ensure that we are a globally competitive environment for investment into the research community, as well as in startups and scaleups, from their early research and development phases through to commercialisation.

As part of this framework, Stone & Chalk Group has played a catalytic role in enabling the growth of startups and scaleups across Australia. Our initial focus began in fintech, where we helped facilitate the growth of that ecosystem, seeing the emergence of iconic fintech players.

More recently, we have been growing a more holistic emerging technology ecosystem including: cyber security, web3, artificial intelligence, quantum, proptech, climate-tech, medtech, agtech, and other scaling businesses with novel products and global ambitions. Further information about Stone & Chalk can be found here: https://www.stoneandchalk.com.au/resources/.

As part of this growth, AustCyber merged with Stone & Chalk Group in February 2021, consistent with the previous Australian Government's request for Industry Growth Centres to establish a pathway to be financially sustainable. This merger affirms our confidence in the next phase of the evolution of the Australian cyber security sector. Since that time, AustCyber continues to undertake important initiatives to help grow the sector in Australia.

General comments

In October 2022, we welcomed the 2022-23 Federal Budget measures contributing to the growth and future of our Australian economy. These require a strong skills pipeline, which is the biggest risk for Australia as we transition our economy from fossil fuels to sustainable technologies.

While the Government showed restraint in its 2022-23 Federal Budget, there is an opportunity for the Government to lean into the emerging tech startup and scaleup community that are critical to the future of our economy to help it deliver on its commitments. In this regard, we would like to work closely with the Government and key stakeholders to ensure that these initiatives are well-designed and implemented effectively.

The forthcoming 2023-24 Federal Budget presents an opportunity for the Government to develop a more ambitious innovation agenda, including direct public investment in innovation ecosystem builders to support the development of an inclusive innovation career path for all Australians. We would welcome government assistance directed towards experts that can enable this, avoiding the Government having to pick winners.

There should be a national focus and long-term vision for a sustainable tech-driven economy, which is critical to our future global competitiveness. A strong national innovation ecosystem will lead to more job opportunities that contribute to our economy and well-being and enable Australian businesses to become more globally competitive in the long term.

In this regard, areas that we cover in our 2023-24 Pre-Budget submission relate to the following topics:

1. Innovation
2. Cyber security
3. Talent
4. Industry growth and sustainability
5. Environmental sustainability

Summary of recommendations in this submission

Topic	Recommendations
1. Innovation	• To ensure that the objectives of any innovation and industry development related initiatives announced through the Federal Budget are properly implemented, the Government and innovation ecosystem builders need to work closely earlier and supported with appropriate funding to execute these initiatives effectively. • A national innovation strategy should be developed, bringing together various initiatives and stakeholders across government agencies and Australian jurisdictions. This should be done in close collaboration with innovation ecosystem builders. Not limited to coordination or integration of initiatives, the strategy should also properly define the problem statement and objectives, develop programs that address the problems and objectives, develop proper measures of success, and properly identify stakeholders that will be required to implement government programs and properly fund these stakeholders. For example, industry and universities will be key stakeholders to help deliver effective programs. • A genuine holistic entrepreneurial career pathway for accelerators and a more curated innovation ecosystem are essential to help startups and scaleups to have increased chances of success to grow and be sustainable in Australia. To enable greater access to our innovation community, we are currently in discussions with various government agencies and private sector entities for their support to expand our national footprint across Australia, as well as global footprint. If well-designed, there will also be wider community benefits in providing easier access for those in currently under-served regional areas and socio-demographic groups. Federal Government assistance in this area would be more than welcomed.

Topic	Recommendations
2. Cyber security	• Government investment in the cyber security sector has been critical to date. Given the industry's infancy in Australia compared to other more established sectors, it is important that the cyber security sector (especially startups and scaleups) receive ongoing support in growing their businesses. • Early-stage funding in Australian cyber security startups and scaleups should be increased to improve their international competitiveness, supported by access to a larger venture capital market and government investment. • R&D government funding support for cyber security should be increased to be more comparable with other emerging tech investments such as AI in the Australian Research Council (ARC). However, caution needs to be given against prioritising between emerging technology investments. • Cyber security uplift support continues to be critical for entities, especially those subject to the recent amendments made to the Privacy Act, as well as the wider range of businesses captured under the Security of Critical Infrastructure Act. This also extends to smaller businesses including those along the supply chain. Support could include investment in domestic cyber security solutions to improve cyber security maturity and capabilities of businesses in accordance with relevant cyber security standards.
3. Talent	• Processing of applications for skilled tech workers under the permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa should be benchmarked against our international peers. • Processing of critical visa applications should be extended to cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers. • Additional measures to address the backlog of skilled worker visa applications should be explored such as increasing funding support for accelerating the processing of applications and reducing wait times. This may be in the form of recruiting more public service workers and procuring technologies that will expedite the processing of applications. • A specific attraction campaign should be conducted specifically targeting cyber security and other high tech specialist talent overseas in order to increase the quantity and quality of applicants in Australia.

Topic	Recommendations
	• Appropriate government funding should be allocated to bridge diversity and inclusion initiatives that enable access to talent with building innovation ecosystems and cyber security capabilities across Australia. • Our education system requires ongoing reform to ensure it develops a longer term pipeline of talent, and responsive to the continually evolving emerging tech environment. This should start early at schools and be co-designed in partnership between schools, industry and governments to build effective school programs around entrepreneurship, innovation, and cyber security and cyber safety. This could entail prioritising appropriate government funding of industry-school partnerships in these domains.

4. Industry growth and sustainability	• As the Future Made in Australia Office establishes itself, we look forward to working with the Government to ensure that procurement of solutions from startups and scaleups, especially in the emerging tech space, are properly supported to succeed and help the Government achieve its procurement policy objectives.
	• Further government investment should be given to the following areas:
	  ○ Collaboration and coordination between the various Australian government jurisdictions and agencies and industry stakeholders on global trade support activities to raise awareness of how we can collectively assist companies to export. This covers our different regions of government and areas of government focused on cyber security and other enabling emerging tech.
	  ○ Promote better the success stories of domestic emerging tech businesses that have been able to export and unpack how they have done so well, and lessons that their peers could learn from those journeys (warts and all).
	  ○ Industry and government working closely on how to support and deliver successful trade delegations and missions around the globe for cyber security and other enabling emerging tech.
	  ○ Investigate how the challenges of domestic security responses to cyber security and national security (e.g., amended SOCI Act and Privacy Act) can be turned into a positive opportunity to create a competitive advantage for our domestic cyber security capability that can be

Topic	Recommendations
	converted into our global comparative strength. ○ Further explorations about the implications of free trade agreements between Australia and other countries that strengthen our trade ties that could flow onto our emerging tech businesses. ○ Explore integrating government trade support with domestic government procurement to strengthen government promotion of exports. This should provide a demonstrated form of assurance by the Government for the companies that they are seeking to promote (subject to appropriate probity and procurement rules).
5. Environmental sustainability	• We welcome working with the Government on its various programs that will support investment in emerging tech solutions as a critical component to transitioning to a cleaner energy ecosystem in Australia.

Should the Treasury have any questions regarding this submission, please do not hesitate in contacting our Director, Government Relations & Policy Advocacy, Charles Hoang. He can be reached directly at charles.hoang@stoneandchalk.com.au or on 0402 096 756.

Yours sincerely

Michael

Michael Bromley
Chief Executive Officer
Stone & Chalk Group

1. Innovation

With Australia's overall ranking of 25th (out of 132 countries) in the Global Innovation Index (GII) 2022, there is much room for improvement on Australia's innovation performance to be competitive amongst its international peers.[1] This requires increased economic complexity, driven by the creation of new products and services, diversification of industries, and enabled through a tech driven economy, leading to increased economic growth and development. This is becoming a more pressing issue as Australia's innovation performance has declined and remained at this level over the last several years.

The forthcoming 2023-24 Federal Budget presents an opportunity for the Government to develop a more ambitious innovation agenda, building on the previous 2022-23 Budget.

Announced in the 2022-23 Federal Budget, the new Startup Year Program offers a promising investment of $15.4 million over four years to allow up to 2,000 University graduates and undergraduate students to learn the fundamentals of being part of the startup community. This is an excellent opportunity to expose graduates to the career opportunities of founding an emerging technology company. We look forward to working with the Government and universities to implement an effective program. Looking beyond the tertiary level, more support will be needed to support our wider education system (discussed later).

The establishment of the Government's $15 billion National Reconstruction Fund will support, diversify and play an essential role in transforming our economy through targeted co-investment support for Australian Industry. We also look forward to working with the Government to ensure that the Fund can help drive growth in Australia's emerging tech industry. This is an area that could help to improve our GII 2022 ranking in investment, with Australia ranking 28th on finance for startups and scaleups, and 31st on venture capital received (value, % GDP).

There were also a range of important initiatives announced in the 2022-23 Budget associated with energy and climate change, defence industry development, foreign affairs, digital infrastructure and connectivity, and investment in regional Australia. There is an opportunity to

[1] https://www.wipo.int/pressroom/en/articles/2022/article_0011.html

embed the startup and scaleup emerging tech community as important contributors to our developing industries, which can be enabled by these government announcements.

Notwithstanding these positive initiatives, there are important opportunities to build our innovation agenda further. For instance, there are various initiatives associated with innovation covering a range of aspects under various labels e.g., critical technologies and emerging tech initiatives, R&D commercialisation, entrepreneurship, Industry 4.0 etc. The challenge is that these activities can be fragmented and disconnected. Sometimes it seems that it would be easier to achieve coordination than integration between these initiatives. This is not limited to one jurisdiction but across Australia.

As a not-for-profit, our core business is to create an ecosystem for helping startups to build their businesses, from pre-startup all the way through to enterprise, giving them access to capital, infrastructure and guidance. During their journey, we provide Founders and their businesses with guardrails to enable them to scale. By our intended design, we offer a genuine holistic entrepreneurial career pathway for accelerators and a more curated innovation ecosystem. This is our approach to addressing disconnected innovation programs.

This is the challenge for many well-intended publicly funded innovation and acceleration programs. They are created as point-in-time programs with a specified duration period, but do not offer any direction or connection beyond the life of the expiry period for that program. Applicants that enter the program are then left to their own devices after the end of the program. Without proper integration into an innovation ecosystem, applicants have an increased chance of failure and therefore are less likely to become sustainable beyond the program. This then raises questions about the value for these publicly funded programs.

To enable greater access to our innovation community, we are currently in discussions with various government agencies and private sector entities for their support to expand our national footprint across Australia, as well as global footprint. If well-designed, there will also be wider community benefits in providing easier access for those in currently under-served regional areas and socio-demographic groups. Federal Government assistance in this area would be more than welcomed.

With improvements in areas such as those discussed around strengthening our innovation ecosystem, Australia has the chance to become more globally competitive, driven by a more innovative economy. These may also help to target some of our weaker innovation indicators highlighted in the GII 2022 such as in entrepreneurship policies and culture (ranked 37th), and state of cluster development and depth (ranked 36th).[2]

Recommendations:

- To ensure that the objectives of any innovation and industry development related initiatives announced through the Federal Budget are properly implemented, the Government and innovation ecosystem builders need to work closely earlier and supported with appropriate funding to execute these initiatives effectively.

- A national innovation strategy should be developed, bringing together various initiatives and stakeholders across government agencies and Australian jurisdictions. This should be done in close collaboration with innovation ecosystem builders. Not limited to coordination or integration of initiatives, the strategy should also properly define the problem statement and objectives, develop programs that address the problems and objectives, develop proper measures of success, and properly identify stakeholders that will be required to implement government programs and properly fund these stakeholders. For example, industry and universities will be key stakeholders to help deliver effective programs.

- A genuine holistic entrepreneurial career pathway for accelerators and a more curated innovation ecosystem are essential to help startups and scaleups to have increased chances of success to grow and be sustainable in Australia. To enable greater access to our innovation community, we are currently in discussions with various government agencies and private sector entities for their support to expand our national footprint across Australia, as well as global footprint. If well-designed, there will also be wider community benefits in providing easier access for those in currently under-served regional areas and socio-demographic groups. Federal Government assistance in this area would be more than welcomed.

[2] https://www.wipo.int/edocs/pubdocs/en/wipo_pub_2000_2022/au.pdf

stone& CHALK
Together we ideate. innovate. impact.

2. Cyber security

2.1 State of the sector

In the most pressing time of our nation's cyber security history, with a cyber-attack occurring every two minutes (and expected to double by 2027),[3] we are facing a critical time to grow Australia's cyber security industry and protect our wider economy. A sustainable cyber security sector will be a critical enabler to strengthening our emerging tech and wider industry.

Government investment in the cyber security sector has been critical to date. For example, since its inception in 2017, AustCyber has played an important role in the progression of the Australian cyber security sector. Driven by the mission of growing, exporting and education, AustCyber has aided the development of a vibrant and growing network of Australian-based cyber security businesses. Today, there are an estimated 291 businesses in the sector.

Given the recent context of our nation experiencing some of the most serious cyber attacks in our history, while unfortunate, this news was a timely reminder for all. We have also separately seen an amendment to the Privacy Act (including an increase in the maximum penalty for serious privacy breaches by up to $50 million) and the Federal Government announcing reforms to the migration system and a comprehensive review of Australia's Cyber Security Strategy. And during the keynote opening address at AustCyber's flagship event, Cyber Week 2022 (held from the 14th to 18th November 2022), Minister for Home Affairs and Minister for Cyber Security, the Hon Clare O'Neil MP, announced that Australia was leading a global ransomware task force, which brings together a group of 37 countries who are all concerned about and experienced ransomware attacks.

All these recent government announcements indicate that as a nation, we are taking cyber security more seriously than ever before. Not just locally but on a global scale, focusing on changes and initiatives that will help grow Australia's cyber security profile and capabilities across the entire world.

However, according to the 2022 Sector Competitiveness Plan (SCP) launched during Cyber Week 2022, we have a long way to go if we want Australia to - not only gain a reputation of being the

[3] According to AustCyber 2022 Sector Competitiveness Plan (SCP), https://www.austcyber.com/resources/sector-competitiveness-plan

most cyber secure nation in the world, but also - strive for a more ambitious goal as a global cyber security super power.[4] Since the release of the SCP, we have seen major government announcements made to strengthen our cyber security capabilities globally, but we are still witnessing fundamental concerns that need to be addressed with urgency and priority. Ongoing government support is therefore critical.

According to the SCP, the annual revenue growth of the Australian cyber security sector has averaged 8.7% over the past five years, significantly slower than other leading cyber security jurisdictions that have inadvertently grown as a result of geopolitical tensions, ecosystem benefits and strict regulations. Underspending in Australia across several key areas has seen a less globally competitive cyber security sector, diminishing our sovereign capability, and presenting both an economic and national security risk. However, Australia has an opportunity to add $800 million to annual cyber security revenue by 2026[5] and catch up with our international peers. This will require immediate focus and investment in the sector.

The SCP also found that cyber security startups in Australia generated 300 times less funding than their international peers, especially in early-stage funding. This is a deep concern for a relatively young industry in Australia that is trying to scale. An additional disadvantage is our comparatively small and immature venture capital market and lack of government investment funding compared to our overseas counterparts.

We note that cyber security is an important subject that will be reviewed as part of the Cyber Security Strategy Review. Notwithstanding this, our SCP and expert feedback received during Cyber Week 2022 highlight several key areas that would benefit from immediate action to grow a more competitive cyber security sector.

Below are further recommendations to help boost our cyber security sector (in addition to areas relating to improving exports, procurement and talent, covered elsewhere in this submission).

[4] The SCP is designed to help shape, inform and grow Australia's vibrant and globally competitive cyber security sector. The 2022 SCP explored themes that are fundamental to the sustainability of our cyber security industry for years to come.
[5] https://www.austcyber.com/resources/scp-2022/chapter-3.

Recommendations:

- Government investment in the cyber security sector has been critical to date. Given the industry's infancy in Australia compared to other more established sectors, it is important that the cyber security sector (especially startups and scaleups) receive ongoing support in growing their businesses.

- Early-stage funding in Australian cyber security startups and scaleups should be increased to improve their international competitiveness, supported by access to a larger venture capital market and government investment.

2.2 R&D investment

According to the SCP, R&D government funding support for cyber security decreased by $2.3 million (23%) over the last three years (from $9.8 million in 2019 to $7.5 million in 2022). This is despite the expectations of many that funding should be increasing to meet the evolving cyber security threats to our nation. Interesting to note is that other emerging tech research such as AI received 20 times more investment ($10 million) in 2022, than in cyber security.

There are many emerging technology investment opportunities made available via government funding such as the Australian Research Council (ARC). If funding is being allocated to other critical technologies such as AI over cyber security, this creates a scenario where government funded programs are inadvertently "picking winners". As a result, others are losing out.

This unintentionally creates an artificial dichotomy between emerging technologies, where they should instead really be given equal opportunity to dynamically cross-pollinate and produce innovative solutions. For instance, AI and quantum technologies have featured in cyber security solutions through diversity of ideas. Cyber security should be a foundation for many of our emerging tech startups and scaleups to give them a competitive advantage. If venture capitalists struggle in picking winners, it would be difficult to expect government programs to be any different. Caution therefore needs to be given against prioritising between emerging technology investments, especially in the area of R&D.

The lack of R&D investment in the cyber security sector further translates to difficulties for our cyber security businesses to sell their homegrown products to local as well as overseas companies and governments. During Cyber Week 2022, we heard about cyber security

companies that have tried to export overseas but are commonly faced with questions from prospective overseas clients to prove their legitimacy and credibility by demonstrating local procurement and investment. If they are not supported locally, it becomes a potential barrier for accessing export markets as well. While government support for business trade activities is welcomed, governments can also explore procuring these businesses to improve their trade prospects.

Recommendations:

- R&D government funding support for cyber security should be increased to be more comparable with other emerging tech investments such as AI in the Australian Research Council (ARC). However, caution needs to be given against prioritising between emerging technology investments.

2.3 Cyber security uplift

At the boardroom level, cyber security and technology literacy more generally has been discussed for a while now. With growing public expectations and government regulatory responses to recent major cyber security incidents and data breaches, it is anticipated that this might shift boardroom discussions to reconsider the value of cyber security, making boardroom leadership in cyber security even more critical.

However, cyber security is traditionally perceived to be a cost centre for many businesses rather than a value proposition (and therefore not a revenue generator). This is despite the fact that cyber security is about managing risks and ensuring business continuity that in turn generates revenue. If this view is translated into wider perceptions about cyber security investment, as highlighted during Cyber Week 2022, it is critical we shift the focus of cyber security from being considered a cost centre and a reactive measure, to being an enabler for growing businesses.

With recent amendments made to the Privacy Act, increasing the maximum penalty for privacy breaches by entities, there remains the practical question of how these regulatory responses will directly drive best privacy and cyber security practice and mitigate such incidents from occurring in the first instance. Along a similar vein are the amendments to the Security of Critical Infrastructure Act, which saw a wider range of sectors and entities subject to new security obligations, including cyber security.

Indeed, everyone has a role to play in securing our businesses, community and nation. Introducing regulations - although well-intentioned - greatly assumes everyone, especially key decision makers in organisations, are fully equipped with the requisite knowledge to invest in appropriate measures to uplift their cyber security in accordance with relevant cyber security standards.

Although governments play a key role through various key agencies like ACSC, CISC and AFP to assist entities on cyber security incidents, industry also has an important role to provide cyber security uplift. In this mix, there are opportunities to encourage the investment in and procurement of services and products from the Australian cyber security sector. If appropriate incentives are in place, there is a huge opportunity for the government to bridge the gap between regulatory measures and wider investment in our sovereign cyber security capabilities. This in turn will also help affirm and promote the credibility and value of our Australian cyber security businesses, improving export opportunities to prospective overseas clients.

Recommendations:

- Cyber security uplift support continues to be critical for entities, especially those subject to the recent amendments made to the Privacy Act, as well as the wider range of businesses captured under the Security of Critical Infrastructure Act. This also extends to smaller businesses including those along the supply chain. Support could include investment in domestic cyber security solutions to improve cyber security maturity and capabilities of businesses in accordance with relevant cyber security standards.

3. Talent

To support a sustainable innovation ecosystem, we need to have access to a sustainable pipeline of talent and skills to meet the demands of the emerging high-tech industries, from early school age to the workforce.

It is widely recognised that Australia is facing a growing skills shortage across our industries. But we are not alone. This is a global problem, amplified by the pandemic. This is leading us to a global race for not just more people, but the right people, with the right training, at the right time, and in the right places.

Unless appropriate action is taken very soon, there is a risk that Australia will fall further behind its international peers, and we will be discussing the same problems but further amplified, in years to come.

The Jobs and Skills Summit consultations by the Treasury, as well as review of the migration system by the Department of Home Affairs, presents a critical opportunity to address the talent challenges.

To develop properly targeted policy solutions, this needs to be supported by relevant data.

For instance, our recently released AustCyber 2022 Sector Competitiveness Plan (SCP) reported that there will be 3,000 fewer cyber security workers than required by 2026. The SCP highlighted that our talent shortage dilemma is a result of projected inflows and outflows from the cyber security workforce. Although there are more people entering the sector, with enrolments and skilled migration numbers growing (albeit at a much slower rate compared to before COVID-19), this is not fast enough to keep up with attrition from the sector and increased demand.

There will be current cyber security workers who will eventually leave the workforce, including those workers retiring and others moving to other industries. Although the SCP estimated an increase in new graduates, upskilled and reskilled workers, and skilled migrants will likely replace workers leaving the workforce, projected demand for cyber security workers by 2026 is estimated to exceed supply. This issue is likely to be not limited to the cyber security sector.

For highly specialised areas such as in cyber security, Australia will need a large number of experienced workers with more than six years of deep industry expertise. These will be highly technical roles, requiring a three-year university degree, and at least another three years of on-site experience. This experience would include recognising, reacting and managing cyber security incidents.

This expertise issue is not limited to cyber security, but also data management, software engineers and developers. Without the requisite talent, organisations will lack the appropriate capabilities to either anticipate or respond to a cyber security attack, leading to increased vulnerabilities.

This means the issue cannot be solved in the short-term labour market by adjustments or training. Addressing the problem therefore requires a two-phased approach. Firstly, skilled cyber security migrants will be required to quickly address the immediate organisational vulnerabilities. Secondly, our education system will need to be bolstered to ensure we have an ongoing pipeline of talent to draw upon to manage the continuously evolving cyber security threat landscape.

3.1 Skilled migration

Skilled migration will further bolster our own efforts through the sharing of knowledge, reinforcing the education pipeline by solidifying the skills of emerging tech graduates. This will be especially important in cyber security who will serve as the first barrier to would-be attackers for years to come. Akin to how Australia has approached the education and healthcare sector skills shortages, we need to meet the current and future demand in emerging high tech jobs with highly skilled foreign workers.

In addition to acquiring critical overseas talent and migrating them to Australia, it is also important to ensure retention of talent through incentives. Our migration system will need to be cognisant of the competition for talent, not just between the various sectors, government and private sector domestically, but around the world. Overall, our system will need to be conducive to enticing and retaining talent, rather than creating unnecessary barriers.

There are barriers that can be immediately resolved through government reforms, especially in light of the competition in the global jobs market. In particular, the current migration protocols and wait times need to be quickly adjusted to ensure Australia is a viable candidate for any

international expert looking for new opportunities in new places, and do not fall behind in the highly competitive global race for tech talent.

For example:

- Australian visas for the tech industry take much longer to process compared to our international peers. The permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa currently take between three and six months to process. In contrast, the current approval process for skilled tech workers in New Zealand takes 20 days, 15 days in the United Kingdom, and 10 days in both Canada and Israel.

- We understand visa applications have recently been given high priority to healthcare and teaching professions, which are well-deserving and under-resourced.[6] Equally, it is important that processing of critical visa applications including cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers, should be similarly elevated in priority. This has become especially important due to the recent major cyber security and data breach incidents. We understand that the current wait times for these applications may have been significantly delayed.

Recommendations:

- Processing of applications for skilled tech workers under the permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa should be benchmarked against our international peers.

- Processing of critical visa applications should be extended to cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers.

- Additional measures to address the backlog of skilled worker visa applications should be explored such as increasing funding support for accelerating the processing of applications and reducing wait times. This may be in the form of recruiting more public service workers and procuring technologies that will expedite the processing of applications.

- A specific attraction campaign should be conducted specifically targeting cyber security and other high tech specialist talent overseas in order to increase the quantity and quality of applicants in Australia.

[6] https://immi.homeaffairs.gov.au/news-media/archive/article?itemId=973

3.2 Diversity and inclusion

During Cyber Week 2022, significant discussion focused on the underutilisation of untapped sources for access to talent. Experts noted that there were socio-demographic groups that were not being sufficiently considered.

If appropriately harnessed, they could contribute to the talent shortage challenges and provide invaluable economic and societal benefits. Building diverse teams of people from under-served regions and backgrounds, including First Nations people, females and neurodiverse, can boost our innovation and knowledge capabilities to solve problems, bringing with it diversity of lived experiences, skills, values and perspectives. This also includes people who may not follow traditional educational pathways from TAFEs and universities that might have the right skill sets that are also untapped.

Expert feedback during Cyber Week 2022 discussed these barriers as key reasons for Australia's talent shortage. These reasons have been, and still are, also being widely discussed across the country and our economy, including as part of the Australian Government's Jobs and Skills Summit consultations.

Congruent to leadership and culture is implementing diversity and inclusion practices to build and grow an effective team. Examples discussed demonstrate that there are opportunities that can help to boost our talent shortage through these untapped avenues for under-served and diverse groups.

For example:

- Lessons can be learnt from other professions like in engineering to change perceptions around social impact to attract a wider talent pool.
- There are initiatives to support participation in areas like cyber security for people from neurodiverse backgrounds.
- Diversity with respect to gender can be designed and built into daily workplace and practices, as business as usual. Understanding barriers to change plays an important part in improving diversity.

We appreciate that there may be various diversity and inclusion initiatives that exist to support boosting our talent pool, not limited to cyber security. We note that the Jobs and Skills Summit consultations undertaken by the Treasury may be an appropriate avenue to consider this as an important area. Nevertheless, given that Australia is currently facing an immediate skills shortage, urgent action should be undertaken to implement solutions to address our talent shortages in emerging tech, including through diversity and inclusion.

Recommendations:

- Appropriate government funding should be allocated to bridge diversity and inclusion initiatives that enable access to talent with building innovation ecosystems and cyber security capabilities across Australia.

3.3 Education, skills and training

In the longer term, our education, skills and training system will need to be bolstered to ensure we have an ongoing pipeline of talent to draw upon to manage the continuously evolving emerging tech driven economy and threat landscape. The GII 2022 particularly highlights that there is significant room for improvement in our education system for innovation, with a global ranking of 36th.

This starts early at school where students should be taught about cyber security and cyber safety, for example. School-based programs should give schools control in how they deliver it.

One area we would like to see a stronger focus on is adding the "A (Arts)" into STEM, creating STEAM: science, technology, engineering, arts and mathematics. Arts, design and critical thinking are foundational skills that will have a measurable impact on Australia's future workforce and entrepreneurs. It is not just about digital and cyber literacy.

As part of these reforms, teachers are essential and will need as much assistance as possible to ensure they are properly supported (including any training required) to deploy these programs.

Going beyond the school system, our workforce and wider community need cyber security skills. This should not be limited to whether they decide to become a cyber security professional. Our general cyber security awareness should be akin to any form of health and safety, as well as security.

Assistance from governments and industry will be important to develop much needed cyber security education programs that provide an education pathway all the way up to the workforce.

As with diversity and inclusion initiatives, we appreciate that there may be various cyber security and STEAM initiatives that exist to support boosting our talent pool in the longer term. Given that there are talent shortages in the immediate to longer term, compounded by the evolving nature of emerging tech, ongoing investment into our education system is critical.

We note that there are also various government consultations and other activities including the Jobs and Skills Summit consultations undertaken by the Treasury, forthcoming Cyber Security Strategy Review, and Startup Year Program. While these are important consultations, it is imperative that more immediate action is taken to commence implementing longer term solutions.

Recommendations:

- Our education system requires ongoing reform to ensure it develops a longer term pipeline of talent, and responsive to the continually evolving emerging tech environment. This should start early at schools and be co-designed in partnership between schools, industry and governments to build effective school programs around entrepreneurship, innovation, and cyber security and cyber safety. This could entail prioritising appropriate government funding of industry-school partnerships in these domains.

4. Industry growth and sustainability

For businesses to grow and be sustainable, they need access to both domestic opportunities as well as export opportunities.

4.1 Procurement

It is well-recognised that SMEs represent the largest proportion of businesses, as well as the largest employer, in Australia. Ongoing support for smaller businesses is therefore critical to ensure sustainability of our sovereign capability.

Our procurement policy also needs to be designed to be flexible to support less established businesses in the emerging tech startup and scaleup space, not just SMEs more generally. These somehow need to be properly factored in when considering regulatory impact, for example, should we wish to develop sovereign capability for leading edge technologies and the future of the digitally enabled economy in Australia.

We therefore welcomed the Government's commitment to supporting SMEs by updating the Commonwealth Procurement Rules (CPR) in mid 2022 to expand opportunities for SMEs and requiring that 20 per cent of procurements by value are sourced from SMEs.[7] We note that this update to the CPR is an increase from the previous 10 per cent threshold. According to estimates by the Department of Finance, the Commonwealth has well exceeded this threshold at 30.8% in 2021-22, which is positive.[8] Nevertheless, it is unclear from these figures the extent to which startups and scaleups, if any, contribute to government procurement - further clarification from this would be welcomed.

We also support the Government's announcement in the 2022-23 Budget for the establishment of the Future Made in Australia Office as part of its Buy Australia Plan. We note that the initiative is intended to build domestic industry capability and improve access to a wider range of businesses including small to medium businesses. For less established startups and scaleups,

[7] https://www.financeminister.gov.au/media-release/2022/07/01/better-deal-australian-businesses-under-commonwealth-contracts

[8] https://www.finance.gov.au/government/procurement/statistics-australian-government-procurement-contracts-

especially those that are providing leading-edge emerging technologies, it will be important for them to be able to realise these intended benefits in practice.

It should also be acknowledged that at the early stage of these startups and scaleups, they may not always necessarily be considered "value for money" in accordance with the CPR. Therefore, consideration should be given to ensure that building domestic industry capability is not reduced to whether it is "value for money" in the short term. If necessary, exemptions may need to be provided, for example, to incentivise investment in and procurement of solutions from domestic startups and scaleups.

Further, feedback from the startup and scaleup community is that they prefer being a customer to governments and industry rather than just receiving point-in-time grants that do not offer continuity and deeper partnerships. This can be enabled by building a deep connection to local innovation ecosystems and communities, ensuring lessons learned from the past and opportunities identified for the future have the best chance to take hold and build success.

Recommendations:

- As the Future Made in Australia Office establishes itself, we look forward to working with the Government to ensure that procurement of solutions from startups and scaleups, especially in the emerging tech space, are properly supported to succeed and help the Government achieve its procurement policy objectives.

4.2 International trade

With Australia being a small market, it is logical that we have access to export markets to ensure a sustainable pipeline for sovereign industrial capability. We need to move on from the language that we punch above our weight and focus more on promoting our tech startup and scaleup successes i.e., marketed to the world as much as we do in tourism.

A key area for Government if it wishes to support companies that are exporting is to also invest in these businesses by way of local procurement. This demonstrates genuine government support and can help businesses to promote themselves with prospective overseas customers.

4.2.1 Cyber security sector example

Some companies reported during Cyber Week 2022 that they struggled to gain traction through local government procurement and felt they had a better chance to prove themselves overseas. It was also not uncommon for some of these companies to be asked by overseas government prospects if they could demonstrate their domestic credentials with their local government as a reference.

According to the 2022 SCP on our export findings:

- Australia's cyber security sector revenue growth has been significantly slower than other leading nations because of our insufficient focus on export markets.
- Australian cyber security businesses receive a significantly smaller share of revenue from exports when compared to other international businesses.
- Despite cyber security products and services being well-suited to exporting (especially given the cross-border nature of cyber security threats), to date Australian businesses have not been successful in capturing this attractive global market.

Our findings suggest that Australia is small, and a large proportion of cyber security is supplied from somewhere else in the world. Given the Australian cyber security industry is largely made up of small businesses, which includes startups and scaleups, exporting their products and services overseas is considered essential to helping grow and building these businesses to become competitive and successful.

In addition, Australian cyber security businesses that only focus on the domestic market have a small serviceable market. Focusing on serving local demand only offers very limited opportunities.

There was a collective shared sentiment during Cyber Week 2022 that trade is critical for Australia's success and prospects for growth which has expanded from commodities and other tangible goods to intangibles including in cyber security. Improving our trade prospects will also help build and sustain our talent pipeline and, in turn, our sovereign capability.

Despite the generally understood reasons for businesses needing to export, this raises questions as to why Australian cyber security businesses are not taking advantage of the export opportunities, with less than half of them even trying to sell overseas.

Several reasons were touched upon during Cyber Week 2022 including: fear or lack of knowledge or confidence; lack of support; lack of funding; nature of service based vs products based businesses; and the tyrannies of distance and relationships from our global trading partners. So, while there may be accelerated digital transformations and expected corresponding cyber security investment, we have not seen a correlation to growth via exports.

As highlighted in the 2022 SCP, critical and immediate actions are required to overcome our export growth barriers, bolster our export capability, and give Australia an opportunity to add $800 million to annual cyber security revenue by 2026. These include supporting our domestic procurement of cyber security and maintaining and strengthening the sectors' global export-oriented outlook.

Echoing our SCP findings, Cyber Week 2022 discussions highlighted that we need to invest in continued trade outreach programs, including trade delegations, export support and study tours. These can be improved upon through increased collaboration between the various government agencies, and more strategically targeted delegations and groups.

There is certainly no reason why Australia should differ from other countries in terms of cyber security threats, and geopolitical and supply chain challenges. This leads to further questioning of sovereign industrial capabilities and international trade partnerships. Australia has also seen stricter regulations introduced over the last several years associated with national security.

As raised during Cyber Week 2022, there are other opportunities through other government initiatives that should be explored further to support cyber security exports such as the AUKUS trilateral partnership, various free trade agreements, and other global security partnerships such as the Quadrilateral Security Dialogue and Five Eyes Alliance.

The Australian brand in general is globally recognised as trustworthy and reliable. Many international partners would want to be associated with this brand. Awareness of this brand value and our sovereign competence in cyber security may not be sufficiently clear. We should therefore aim to better align and promote our cyber security sector with that trusted Australian brand.

4.2.2 Wider emerging tech sector

Although the SCP and Cyber Week 2022 focused on the cyber security sector, we suggest there are likely to be similar issues for other emerging tech sectors as well. The indicators in the GII 2022 also suggest more room for improvement in various areas relating to our exports, including

Australia's high-tech exports (% total trade) ranked 59th globally, ICT services exports (% total trade) ranked 78th, and creative goods exports (% total trade) ranked 58th.

There are mutual benefits in building cyber security capabilities into other emerging tech industries as global leaders and become Australia's unique value proposition for emerging tech exports. An inadvertent benefit of the amended Security of Critical Infrastructure (SOCI) Act is that it can help drive more local cyber security business investment and capability, leading to comparative advantages overseas.

There are several examples of initiatives such as those offered by AustCyber and Austrade[9], directly targeted at supporting cyber security and other types of businesses to export overseas. There are also other opportunities that can be leveraged through international trade activities between governments, especially in our Indo Pacific region, AUKUS, Quad Alliance, and Five Eyes Alliance.

Notwithstanding these opportunities, there are always areas that could be improved such as how to effectively communicate, connect, coordinate and partner with like-minded organisations and government bodies to support our emerging tech industry.

Recommendations:

Further government investment should be given to the following areas:

- Collaboration and coordination between the various Australian government jurisdictions and agencies and industry stakeholders on global trade support activities to raise awareness of how we can collectively assist companies to export. This covers our different regions of government and areas of government focused on cyber security and other enabling emerging tech.
- Promote better the success stories of domestic emerging tech businesses that have been able to export and unpack how they have done so well, and lessons that their peers could learn from those journeys (warts and all).
- Industry and government working closely on how to support and deliver successful trade delegations and missions around the globe for cyber security and other enabling emerging tech.
- Investigate how the challenges of domestic security responses to cyber security and national security (e.g., amended SOCI Act and Privacy Act) can be turned into a positive

[9] See Austrade's recent insights, "Australia's A$7 billion cyber security opportunity": https://www.austrade.gov.au/news/insights/insight-australia-s-a-7-billion-cyber-security-opportunity

opportunity to create a competitive advantage for our domestic cyber security capability that can be converted into our global comparative strength.

- Further explorations about the implications of free trade agreements between Australia and other countries that strengthen our trade ties that could flow onto our emerging tech businesses.
- Explore integrating government trade support with domestic government procurement to strengthen government promotion of exports. This should provide a demonstrated form of assurance by the Government for the companies that they are seeking to promote (subject to appropriate probity and procurement rules).

5. Environmental sustainability

We welcomed the Government's 2022-23 Budget announcement of various climate and energy transformation initiatives targeted at investing in cleaner, cheaper and more secure energy, creating jobs and spurring investment in new energy industries, and reducing emissions and addressing climate change. These form part of the Government's Powering Australia Plan.

From a climate change and energy perspective, there is an opportunity to invest in cleaner and sustainable emerging technologies that can greatly contribute to the Australian Government's ambitious emissions reduction target by 2030 and beyond. If invested properly, we have an opportunity to establish Australia as a climate change leader through the transition to a sustainable, tech-driven economy. This can also improve our innovation performance where our standing on ecological sustainability was ranked 47th in the GII 2022.

As the world becomes more focused on sustainability, countries that fail to adopt new emerging technologies and practices will fall behind in terms of competitiveness, and Australia must stay ahead of the curve. This way Australia can be a leader in the field of climate tech and attract more investment in sustainable projects.

To achieve this progression over the next decade, obstacles facing all forms of emerging technology initiatives need to be removed, including lack of early-stage funding, minimal regulatory support, and limited investment in emerging technology solutions. We need an established, clear pathway that allows climate tech companies to finish what they started without falling victim to one of the many obstacles that may arise in their way.

Areas that will need ongoing public support and focus on include:

- Investment in research and development in emerging climate tech
- Incentives for companies to invest in emerging climate tech solutions
- Investment in infrastructure to support the growth of emerging climate tech
- Support for startups and scaleups working on emerging climate tech to help them grow and commercialise their products and services
- Education and training programs to build workforce capability to support the growth of emerging climate tech in this space
- Support public-private partnerships to accelerate the growth of emerging climate tech in environmental sustainability

Recommendations:

- We welcome working with the Government on its various programs that will support investment in emerging tech solutions as a critical component to transitioning to a cleaner energy ecosystem in Australia.