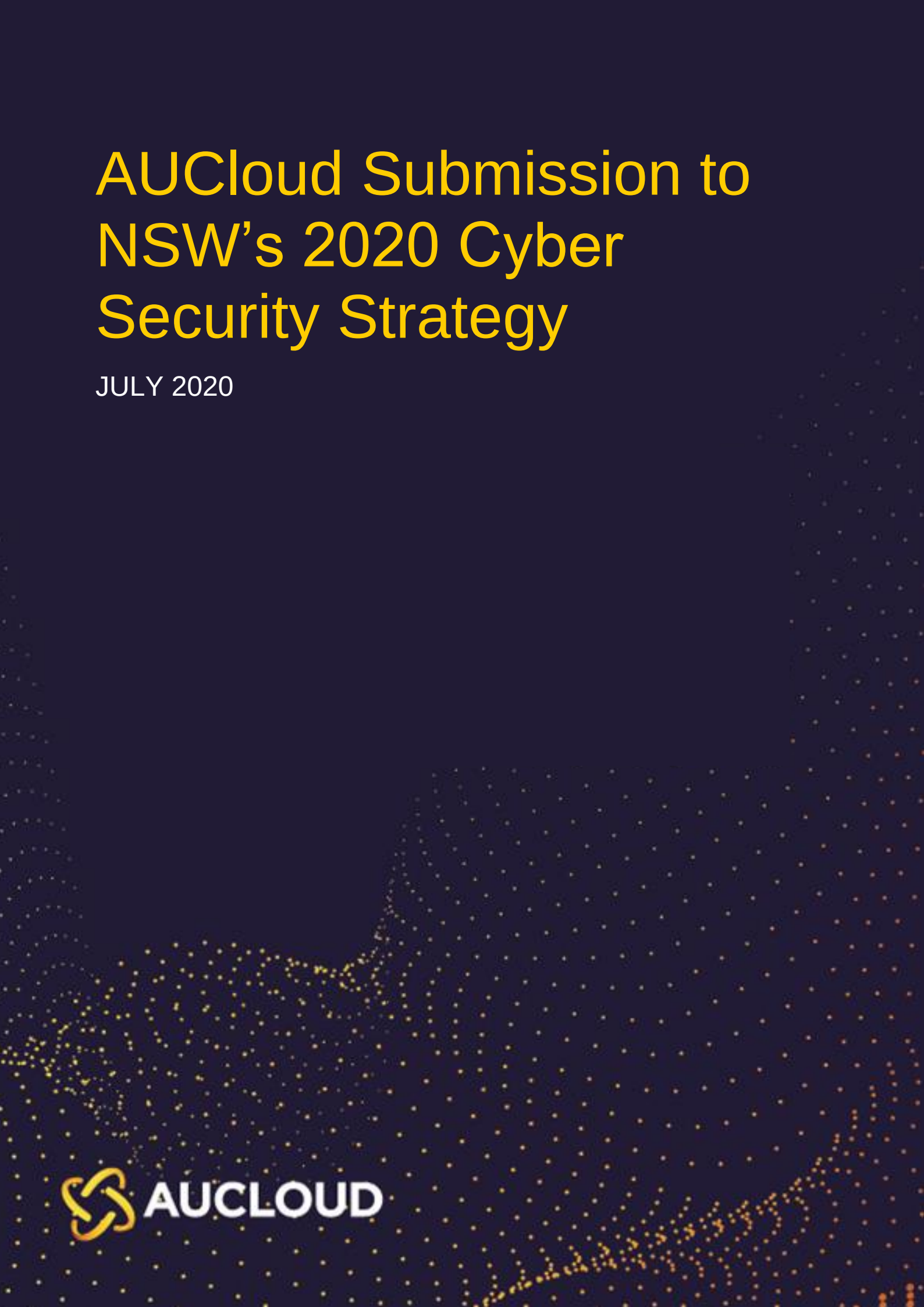
AUCloud Submission to NSW's 2020 Cyber Security Strategy

JULY 2020



Disclaimer

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

Introduction

Thank you for the opportunity to respond to the **2020 NSW Cyber Security Strategy**.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the needs of the Australian Government and Critical National Infrastructure (CNI) communities. This includes Federal, State and Local Governments and CNI organisations such as telecommunications, electricity, energy, financial services and similar utility providers.

Security is core to how we operate at AUCloud.

Independently IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM), AUCloud provides two independent environments: an Official Data Community Environment (ODCE) and a PROTECTED Data Community Environment (PDCE) that meet or exceed these controls.

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

AUCloud operates from two Data Centres: Sovereignty Zone 1 in Canberra and Sovereignty Zone 2 in Sydney, both designed to meet ASIO T4 standards for Zone 4 security.

AUCloud Submission - NSW Cyber Security Strategy

AUCloud submits the following response to the 2020 NSW Cyber Security Strategy – noting that organisations have the option of replying to all or some of the questions posed.

Resilience

1. **What role should industry, government and the public each have in increasing our overall cyber security resilience in NSW?**

Government has a lead role to play in building cyber resilience. However, if the Government is to assume a lead role it must ensure that it is appropriately positioned to quickly respond to and address serious threats. While the ACSC has been established at the Federal level and can assist with nation scale threats, the industry is seeking more proactive involvement and leadership when it comes to real time incident response activities across a much broader range of issues than just nation scale threats.

Being able to provide rapid response and assistance to NSW businesses should be a key deliverable of the Cyber Security Strategy. Similarly, any rapid response capability should be tested across a variety of sectors without focusing specifically on a small test group. Such an approach would require enhanced levels of investment to address a much wider threat vector and protect those that have invested in NSW.

A greater focus on building systems that are on well protected sovereign platforms, where all data, meta-data, monitoring data and derived data, are guaranteed to remain in Australia under Australian law and away from external jurisdictions would further simplify complex matters when dealing with cyber security incidents.

It is no secret that many NSW businesses are completely unaware of the contractual details they enter with global providers and the Government has long talked about promoting and enhancing the IT and cyber security sectors. A renewed Cyber Security Strategy presents a prime opportunity to further highlight the need for sovereign capabilities.

In addition, establishment of an incident response marketplace (perhaps as part of buy.nsw), operated by a NSW Government entity or possibly in conjunction with the Australian Cyber Security Centre (ACSC) and entered into based upon zero-dollar contracts, would also alleviate a common problem of who to seek assistance from when dealing with a cyber security incident. Organisations that AUCloud engage (customer, partners, supply chain, etc) often highlight this as an issue they have faced; especially the inability to distinguish one incident response capability from another, with business decisions primarily based upon financial decision making.

2. **Should the NSW Government play an involved role in increasing the individual cyber resilience of NSW citizens and business? If so, how?**

The Government definitely has a role to play. In regard to NSW citizens this will be much harder as people need to remain accountable for their individual decisions, nonetheless, given the rise in cyber crime and issues such as identity theft, awareness campaigns are required that start at a school age and continue all the way through to an elderly age. NSW's Government digital investment and footprint are some of the best in the country but to truly capitalise on these investments an awareness campaign to promote the safety and efficiency of digital is crucial.

Likewise, cyber resilience for businesses is equally important in building trust with NSW citizens. We would encourage the NSW Government to adopt a scheme similar to the UK Government's Cyber Essentials scheme. Cyber Essentials is a simple but effective approach to assisting businesses protect themselves from a wide range of the most common cyber-attacks based upon 5 effective security controls. A similar scheme in NSW, at a non-restrictive price point, would allow a large variety of businesses not only to uplift their cyber security knowledge but also to promote their commitment to cyber security principles.

3. **What are the threats that the NSW Government should be focusing on and what practical steps could be taken to address these?**

As tools for threat actors become cheaper and more readily available, the cyber threat environment will continue to evolve at a rapid pace, often faster than Government and suppliers will be able to respond. The capabilities of nation state actors are well known although their attack surface is, for the most part, restricted to Government outcomes and suppliers. However, the primary target of threat actors will continue to be the theft of personal and financial information of individuals and businesses. Affordable and low-tech attacks such as ransomware, phishing and malware will continue to rise and a greater emphasis from Government on supporting small to medium businesses and corporate Australia from cyber criminals is required. In that sense, for many Australian businesses, a mind-shift to data centric protection and understanding the value of their data would greatly assist risk-based decision making.

Part of that conversation will focus on the threat and ways it can be mitigated but more education is also required to assist these businesses to understand cyber security risks in the first instance. In our view, Government programs have been successful in their own ways but much more can be done by Government to assist businesses in understanding cyber risk levels before identifying specific threats.

We have observed first hand NSW's involvement in the Joint Cyber Security Centre's (JCSC) and believe this has been a welcome addition to filling the communication gap between Government and business on cyber specific topics and would further encourage NSW to enhance these relationships so that businesses continue to receive timely and valuable advice.

The collaboration within these communities is an ideal starting point to further the breadth of Government assistance and involvement against cyber crime. The challenge for NSW will be how to expand and scale these services to assist businesses, and corporate Australia, more broadly.

We would also expect to see more focused attempts from sophisticated threat actors to exploit the trusted relationships between businesses and their suppliers/service providers for cyber crime purposes. Any compromise of the supply chain, especially hardware and software supply chains, will make the detection and attribution of cyber crime more difficult.

4. **What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?**

People often refer to the need for good cyber hygiene which draws parallels to the Work Health and Safety (WHS) improvements over the last 30-40 years. During this time, improvements and changes to the WHS industry have largely been driven by an increase in the better capture of data for both incidents and near misses, as well as significant increases in sanctions (fines and even imprisonment) for organisations that fail to improve.

Cyber security as an industry is still in relative infancy, with many of the mandatory reporting schemes only coming into effect in the last 5 years as cyber security breaches have increased and consumers have demanded greater protection of their information. It is important that as this information continues to be gathered that NSW Government adapts to a changing environment, identifies key areas of concern and implements sufficient legislation, frameworks and penalties for companies that don't maintain sufficient protections or meet the necessary standards for cyber resilience.

5. **How can the NSW Cyber Security Policy be improved in regard to the policy's implementation and robustness?**

Overall the policy is well written and encompasses the required information, as well as several mandatory conditions. One area that could potentially be improved upon within the Cyber Security Policy is the need to identify specific types of data and the level of protection required. We believe that ultimately the NSW Government is charged with the protection, or robustness, of systems that the public relies upon or data that has been shared.

6. **How can inter-government relationships be improved to bolster NSW's cyber security posture and resilience?**

Critical to the success of inter-government relationships is a clear understanding of data flows across Government, including roles and responsibilities in the event of a cyber security incident. We've noted the development of the NSW Cyber Security Incident Emergency Sub Plan and recommend the continued testing (cyber security exercises) of this plan across critical services to bolster NSW's cyber security posture and resilience in the event of a genuine cyber incident.

7. **What strategies should NSW Government use to lead the way in detection and response?**

At a national level, improved technologies such as DNS security (analytics, threat detection and proactive blocking) can be introduced to significantly reduce malicious activity through co-operation with service providers. NSW should position themselves to be a predominant voice in this area, driving for better nation scale security measures.

A Malware Information Sharing Platform (MISP) would also be a significant step to reducing malicious activity while also achieving the objective of rapid response from NSW Government and industry. Approximately 6 years ago the UK Government introduced the Cyber Security Information Sharing Partnership (CiSP) as a joint Government and industry initiative to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, to increase situational awareness and reduce the impact on UK businesses. Such a system should be a high priority as the sharing, storing and correlating of data to detect and prevent attacks, fraud or threats against ICT infrastructures, businesses or people, is mission critical for many organisations.

8. **How can Cyber Security NSW enable the NSW Government to be more cyber resilient?**

By ensuring that cyber security is built-in to digital products and services that the NSW Government provides. It's a genuine commitment to valuing security and building it into goods and services at the beginning. At some point, most likely after a significant incident, citizens will realise the value of those that champion security as part of the goods and services they provide. We envisage that Cyber Security NSW should be the champion of this across NSW Government.

9. **How should cyber security features be prioritised in government procurement of products and services?**

Not sure if they necessarily need to be prioritised but we do believe there should be minimum standards applied to the protection of personal and sensitive information, and that private entities have a responsibility to protect information that is entrusted to them. While this is typically a risk-based decision that varies from one agency to another, a common approach across NSW Government as to what security features, or standards, are required would be a step in the right direction.

Similarly, the threat to supply chains and the risk of theft of intellectual property (IP) and commercially sensitive information is likely to grow in the foreseeable future. There has been significant research in this field to indicate that IP theft is higher when businesses operate abroad – whether that be due to design or manufacturing. Some countries even have domestic policies that allow their Government to access data as it transits or resides in their country. Both Government and businesses should always remain vigilant and aware of how these policies may impact their business.

Within Australia, we can better instill trust in our own procurement processes by developing our own supply chains and investing in sovereign capabilities. As a business, zero trust models should be adopted so that each entity within the supply chain network is required to rely on its own investments and trained staff to mitigate risks to IP and access to data.

Workforce and Skills

10. **Are the workforce and skills initiatives in the NSW Cyber Security Industry Development Strategy addressing the skills gap? If not, what could be done better? What other initiatives could the NSW Government undertake in the area of skills and training?**

We believe they are but like many areas of the ICT sector, technology advancements require these strategies to be reviewed regularly to ensure that they remain current and that the relevant skill gaps are being identified correctly.

13. **How can the NSW Government, educational institutes and industry build a market of high quality cyber security professionals in Australia?**

Many would argue this already exists. If the focus of the question is on developing cyber security professionals for the future it most definitely starts with education. Across Australia, curriculums have started to include cyber security courses at the high school and college levels, significant work has been done at the TAFE level and need for greater emphasis on STEM disciplines is well documented. If Government or private entities wish to accelerate development in these areas, additional investment or greater accessibility should be considered.

Business Growth

15. **What are the barriers for NSW cyber businesses when growing their business?**

By the relatively immature nature of cyber, many cyber businesses are young, often technology start-ups and generally inexperienced in terms of wider financial, commercial and people risk factors associated with building a business. Conversely, cyber businesses also have considerable energy and insights into challenging traditional market structures. However, one of their key challenges is often the decision-making buying cycles of industry but especially government, are far longer than the technology or product development cycles of cyber businesses. This disconnect is also exacerbated by inefficiencies in procurement processes, which require repeated and detailed boiler plate answers about business fundamentals, place too great a weight on longevity and financial performance and require excessive levels of insurance compared with the nature and scale of the procurement being undertaken.

16. **What can NSW Government do to enable business growth and support for cyber security start-ups, scale-ups and SMEs?**

We should start by saying that start-ups, scale-ups and SMEs and not the same.

SME definitions relate to the size of a business often with formal criteria around turnover, assets and/or staffing levels. In our experience, having represented them on a Ministerial committee in the UK, SME businesses by size fall into three very different groups: businesses with 1-5 employees, often single contractor owner or a small family activity, that have little or no ambition of growing, often localised and serving a particular niche or community. Businesses of 6-30 persons who have similar characteristics to the former but have exhibited some form of expansion, maybe across one or two locations/market. The remaining businesses have some sense of ambition but often with some limiting constraint, which could be leadership, financing, risk aversion, addressable market or some other limiting factor.

Start-ups and scale-ups are about ambition levels and are more about the life-stage characteristics. The issue for the start-up is whether there is any ambition to scale beyond the 1-5 stage and potentially grow into a multi-million dollar, growth engine of jobs and exports. Scale-ups, as shown by reports around the world (see Sherry Coutu Sale-Up report UK 2013) are the engine of future jobs and should be the ambition for all governments to nurture. One obvious way to achieve this is for government to use its own considerable purchasing power – not by picking winners, not by handing out grants and favours, but ensuring that in a competitive landscape it ensures the playing field for its local domestic, sovereign providers are as least as level as they are for the shiny glossy foreign subsidiary of an overseas owned provider.

17. **What are the opportunities for cyber in the regional areas? What can NSW Government do to enable more regional cyber businesses?**

Providing the digital infrastructure is fit for purpose, cyber, like all digital technology can be undertaken in virus infected cities or sparsely populated remote regional environments. Hence if government can ensure that the requisite digital infrastructure is in place it can then encourage, incentivise or mandate that cyber activities are undertaken in regional areas of NSW. Critical mass in each regional will require the initial (temporary) migration of technical leaders to provide the core kernel of capability from which longer term (virtual) training and mentoring schemes like OKRDY can establish a more sustainable capability.

18. **How could NSW Government procurement be used to support start-ups, scaleups and SMEs and local cyber businesses?**

See also our response to question 16 for context.

Transparency is THE key facet to establishing an effective and competitive marketplace for any goods and services but especially digital technologies. This means ensuring that all supplier product and service descriptions along with their pricing is available for all to see, including their competitors. This means that all contracts and related expenditure

undertaken by agencies and projects therein are also made visible, which will increase price competition and drive innovation. Economic basics highlight that a key condition for perfect competition is perfect information. At present, much of what government procurement activities achieve on both the supplier and buyer side are causes information to be hidden.

Augmenting transparency with an efficient digital process that reduces costs and removes friction (like buy.nsw), will further encourage the majority of technology organisations across NSW who currently choose not to supply to NSW Government, to reconsider this commercial decision.

You must then trust SMEs (start-ups and scale-ups variants alike) to make the investments in a transparent market to be innovative and problem solve. Many will not but those that do will become the scale-ups of tomorrow and the engines of growth for the country, the region and the world. Governments can spend a dollar and if they are fortunate, they may secure a dollar of value. However, if that dollar is spent on competitive goods and services from a local SME, that dollar will attract $10, $20 or even $100 from the investment community of VCs, Private Equity or superfunds – expanding the company, initiating R&D and creating more jobs for NSW.

Whole of government deals which provide procurement professionals a sense of worth and the vendor a whole new marketing campaign to spruik their services as the chosen solution are not the answer.

Innovation and Research

21. **How can we improve the effectiveness of the current innovation and collaboration initiatives in the Cyber Security Industry Development Strategy?**

We believe that the key strategic themes and initiatives of the 2018 strategy remain relevant in 2020. Having said that, innovation and collaboration require investment and we would like to again highlight the increased value of investing in sovereign Australian businesses for this purpose. It is becoming increasingly important that NSW and Australia require secure and trusted supply chain and industry development will be an ever-increasing component of that supply chain.

22. **Are there specific areas of capability and technical strength that NSW should grow?**

Legacy systems that support and maintain critical infrastructure remain a concern. Supporting industry to enhance the robustness and cyber resilience of critical services is a capability that should be grown.

23. **How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**

Increased consumer focus on cyber security can substantially grow the market and further attract investors and investment in the industry. NSW Government supported bodies such as AustCyber and the State based Cyber Security Innovation Nodes have played a key role in improving the scale, scope and quality of cyber security products and services, as well as being strong supporters of Australian based technology companies.

Other

24. **Are there any other insights or case studies you would like to share?**

The cyber threat environment will continue to change, and we expect threat actors to stay ahead of the game based upon their own motivation, opportunities and capabilities. Many of the tactics, techniques and procedures used by adversaries can be mitigated through awareness and the establishment of cyber security standards. However, defending against cyber-attacks also needs to consider the human element which is most often exploited based upon human behaviour. Addressing these threats requires strategies to not only implement technical controls, but to also build an environment of trust with the wider NSW public that the data they share or hold online, is protected at all times and subject only to Australian law and jurisdiction.

It is important that the outcomes of the 2020 NSW Cyber Security Strategy result in better outcomes for all interested parties, with clear deliverables that make NSW more resilient against cyber-attacks.