

INQUIRY INTO CYBERSECURITY

Organisation: AustCyber
Date Received: 20 August 2020

SUBMISSION

PARLIAMENT OF NSW

PORTFOLIO COMMITTEE NO.1 (PREMIER AND FINANCE) INQUIRY INTO
CYBERSECURITY

AUGUST 2020



Introduction

Changing procurement practices changes the game

AustCyber welcomes the opportunity to provide our perspectives to the Portfolio Committee No.1 – Premier and Finance (the Committee) Inquiry into Cybersecurity. This response specifically relates to the areas of the Terms of Reference about the procurement of services and technology for protecting NSW Government digital networks and services.

Developing strategies to support better partnerships between government agencies and suppliers of sovereign capabilities, both in technology and services, builds on the leadership position the NSW Government has adopted in dramatically transforming its delivery of services. It is becoming increasingly clear that an integrated cyber-physical approach led by governments shows a better way for services transformation, positively influencing secure and resilient uptake of digital activities in other jurisdictions as well as across businesses more broadly.

It is our view that if implemented effectively, the NSW Government's 'Digital Restart Fund', providing for AU\$1.6 billion in facilitated digital activity, will be a game changer for the State and provide a comprehensive model for other States and Territories as well as for partners offshore. Incorporating sovereign procurement, including from smaller providers, is a progressive way to encourage government agencies to think and create different, more user-focused approaches to delivering technology enabled services.

Through what AustCyber refers to as a 'reward for delivery' approach, with agencies only securing follow-on funding by demonstrating successful delivery against project commitments from the previous funding allocation, the NSW Government is driving positive value-based service delivery that is focused on solving dynamic challenges and needs. This will benefit the people of NSW and cement the state as an attractive place to build technology producing businesses and stimulate technological innovation as a high growth economic enabler, driving more high value jobs and sustaining growth for the broader community.

The prioritisation of sovereign cyber security as an area for preferential procurement in governments is key – to meet the security needs of agencies but also to assure security is embedded across all technology types and application as well as the services needed to sustain their application. It facilitates local industry growth and ensures a more level playing field for smaller companies by addressing the inherent advantages larger companies often enjoy. AustCyber has developed what we call a Procurement Sandbox, explained further in this submission, to enable smaller sovereign companies to work closely with government to overcome these advantages and help put these companies on a stronger growth path.



Digital risk to digital trust

Australia has a critical dependency in the digital domain and therefore on the trust and security of all digital activity. With accelerated uptake of digital technologies in response to the COVID-19 pandemic and more day-to-day activities moving online, the data presented and its analysis is an important contribution to the reframing of the nation's approach. Focus is needed on ensuring the digital environment is secure, resilient and effective.

[Australia's Digital Trust Report 2020](#), published by AustCyber in July 2020, argues that key sections of Australia's economy are undergoing a step-change because of rapid transition to a more sophisticated, interconnected digital environment. The Report found that digital activity currently contributes AU\$426 billion to the Australian economy and generates AU\$1 trillion in gross economic output, generating one in six jobs. As the largest economy in Australia, that is proportionately more digitally driven, NSW makes a significant contribution to this national picture.

To underline the importance of digital trust, *Australia's Digital Trust 2020* modelled the economic impact of a four-week digital interruption to Australia's economy, such as through a widespread cyber attack, would cost the Australian economy AU\$30 billion, or 1.5 per cent of Australia's Gross Domestic Product. This is estimated to be equivalent to losing over 163,000 jobs. The economy-wide need for cyber security and resilience is what makes the cyber security sector Australia's true horizontal enabler.

To build and secure digital trust, Australia must continue to invest in the means to secure digital infrastructure and data to not only assure trust but to also sustain efforts to reboot growth. The NSW Government has recognised the importance of building digital trust through cyber security and importantly the need to move from a risk-based approach to an investment approach to strengthen digital resilience both within government and across the state. The June 2020 announcement that it is investing AU\$240 million to bolster the state's cyber security capability and create a world leading industry¹ demonstrates this.

A globally competitive NSW cyber security industry will ultimately underpin the future success of every industry in the state's economy and consequently significantly contribute to the national economy and its global competitiveness. It promotes greater trust in Australia as a safe and desirable place for businesses to pursue digitally driven growth and provides products and services that assure the cyber resilience of all organisations.

Openly linking the work of the NSW Government's ICT/ Digital Sovereign Procurement Taskforce to the development of the next NSW Cyber Security Strategy, together with the work of the Cyber Security Standards Harmonization Taskforce², will ensure outcomes are aligned and digital trust becomes part of doing business with the NSW Government. Further, this will help ensure the supporting policy and procedural frameworks for ICT/ digital sovereign procurement are designed to embed 'secure by design' principles³ and an approach to measured, risk based decision making around ICT and digital procurement is sustained.

¹ <https://www.nsw.gov.au/media-releases/record-funding-for-digital-infrastructure>

² <https://www.nsw.gov.au/media-releases/new-cyber-task-force-to-drive-standards>

³ Such as those recommended by AustCyber in its Cyber Security Industry Roadmap, developed in partnership with CSIRO Futures and Data61, located at <https://www.austcyber.com/resources/industryroadmap>



Building sovereign procurement

AustCyber's response to the Inquiry's Terms of Reference

- (h) *Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:*
- (i) *Provisions relating to cybersecurity generally*

Building sovereign cyber security capability through local skills and businesses is vital to ensure Australian digital activity continues to be resilient and secure. Government can encourage and stimulate growth and innovation in local capability by using its purchasing power to ensure its procurement arrangements recognise and encourage sovereign capability.

Government procurement of sovereign capabilities would benefit from de-risking the business maturity aspects of the provider (where relevant and to the extent possible) and the veracity of the product or service being sought. It would also likely help mitigate potential risks with government being the first customer of early stage companies. Further, developing collaborations between SMEs and government is a significant opportunity to shape and work together on use cases across domains and portfolios that can also provide efficiencies in onboarding or implementation.

AustCyber and its industry stakeholders advocate the following for improving approaches to government procurement, noting much is also applicable to larger industry:

- provide incentives and leverage methods to encourage organisations across the NSW economy to buy Australian first where possible. Other countries such as the United States and United Kingdom do this well and their national security as well as economies have benefited significantly.
- engage with and preference local companies in writing Government tenders, for example, in cyber security capability and put in place multi-party writing teams where project complexity requires or would also benefit from multinational experience. This will ensure the scopes of work have both a large and small organisation perspective. In our experience, Australian cyber security companies have no chance of competing if the specifications are written in ways that automatically discount smaller and medium sized companies to tender. Further, scoping requirements and developing Requests for Tender should be based on requirements and problem statements, not vendor features.
- develop incentives that encourage investment in nurturing and supporting sovereign capability for export through global value chains. Investment in earlier stage technology will create a circumstance for evolving technology to become world class.
- implement AustCyber's Procurement Sandbox which can assist industry to rapidly upskill in supplying to government, as the majority of early stage companies are inexperienced in selling to Government as a customer. The sandbox includes developing measures for de-risking business maturity aspects of the provider by exploring the product or service being sought in the NSW Government's technology environment.

Further, this approach creates a significant opportunity to shape and collaborate on developing use cases. The objective of this approach is for the SME and the government to examine the offered capability, test it in the government's technology systems and support and advise the SME about ways their technology can be improved through strengthening use cases, ramping up suitable certifications, for example.

- overlaying AustCyber's Projects Fund methodology⁴ would provide a unique first step in facilitating the matching of Government problems and challenges to industry capabilities appropriate to respond at a Technology Readiness Level suitable to the agency's context and circumstances. AustCyber can assist facilitating best fit matching of SME capability.

While we are seeing some positive results from combined efforts from AustCyber and industry to facilitate Australian capability into government contracts and engage in related opportunities, it continues to remain sub-scale. The majority of supply of ICT and digital technologies to governments in Australia is largely from offshore markets – it is far from a level playing field⁵. While these markets do have skills and capabilities that are useful here in Australia, fostering local innovation through sovereign procurement arrangements ensures Australia builds its own capabilities for ensuring a trusted Australian digital environment.

Actions stemming from the three-pronged approach underway in the NSW government through the ICT/ digital procurement taskforce, cyber security standards harmonization taskforce and a strategy for cyber security in regional NSW, if implemented holistically, will significantly address these challenges and issues.

(ii) Reporting obligations and the monitoring of cybersecurity incidents

AustCyber supports governments monitoring and reporting cyber incidents and being transparent about the types of threats, how they are changing and where they are targeted. This information is very useful for understanding the threat environment, how it is changing and helping governments, technology and behavioural practices to improve so all organisations can make the necessary changes to protect networks and develop measures to get ahead of the threats and when they arise respond to them quickly to minimise the disruption.

With sovereign cyber security important for creating greater network resilience and digital trust, AustCyber encourages measuring and reporting the level of local procurement that is both local to NSW and Australia in Government contracts currently. This includes understanding the current levels of procurement as well as the areas of ICT procurement where sovereign capability is performing well and where considerable improvement is needed. This will help government focus and target its efforts to improve procurement from sovereign entities and hone its support for smaller providers.

Measuring and monitoring sovereign procurement over time by all agencies and departments will enable the NSW Government to track the performance of its sovereign procurement policies and develop insights on how agencies are adjusting their procurement practices and the nature of the relationships with providers. Consistent with open government practices, making this information available through suitable reporting and tracking will improve accountability and encourage cross government dialogue. This sort of information can be tracked and monitored more easily if reported up into a dashboard and tracked in real time.

(i) The extent and impact of outsourcing of government information systems, including:

(i) Outsourcing to entities which are owned overseas

While AustCyber is not able to comment on the level of sovereign procurement and procurement to overseas entities being undertaken by the NSW Government, as mentioned previously, measuring this procurement and tracking it is important for growing local cyber security capabilities and

⁴ Found at <https://www.austcyber.com/grow/projects-fund/criteria-and-guidelines>

⁵ <https://www.defenceconnect.com.au/intel-cyber/6556-op-ed-sustaining-sovereign-innovation-for-australia-s-cyber-physical-interests>

businesses. Also, AustCyber encourages local procurement for the benefits it drives in innovation, and for growing the local industry with export potential.

In relation to the extent of outsourcing to overseas entities, AustCyber suggests the NSW Government works towards a minimum five per cent sovereign requirement in cyber security related procurements as well as the security components of all technology procurements. This would, for example, unlock tens of millions of dollars in contracting opportunities – a target of 15 per cent with a commitment to grow this year on year as the industry grows would deliver long term sustain benefit for revenue and jobs growth. This target would sit within a recommended overall 25 per cent sovereign procurement target across the NSW Government.

Strict and often inflexible procurement rules oblige many government agencies and private sector companies to engage only providers with a proven track record of fulfilling complex and sizeable security tasks. These internal procedures typically work in favour of large companies, with startups frequently missing out even where there are high level requests by government for larger companies to act as a prime for smaller companies.

Further, the majority of government contracts are considered to be large-value, which are prohibitive for smaller companies to successfully tender for without harming their abilities to service existing customers and or due diligence processes with potential customers. Breaking down contracts into phases where possible, aligned with the 'reward for delivery' approach noted above, would significantly shift this. Large-value contracts is seen as the most significant market hurdle for startups globally.

Research shows, for example, the share of small and medium-sized companies securing government tenders in European Union countries rapidly declines once the overall contract value rises above AU\$150,000. Tender processes could be made more accessible if governments divided their contracts into smaller parcels. Rather than contracting a few very large service providers, they could allow many small companies to service different aspects of their technology needs. Given that purchasing from more providers could also make systems more complex and less integrated, any move to smaller contracts would need to be properly weighed against such potential complications⁶.


Other aspects of public procurement that can also be improved are the panel contract supply arrangements commonly referred to as Standing Offer Notices. These suppliers are pre-approved to do business with the government for a period of several years. While this offers convenience for procurement officers, it limits opportunities for new entrants and often closes off a market because new entrants are not able to apply to join the panel arrangements until they are refreshed, often needing taking years. These panel arrangements also tend to be too cumbersome and onerous for smaller companies to meet. More than this, the long standing arrangements ignore the rapid pace of technology evolution and innovation, locking in the Government to often outdated or less efficient or suitable technologies from the beginning of the procurement.

To address this, AustCyber understands the NSW Government is considering introducing more streamlined accessible arrangements for smaller companies which are more like a registration process. This is a better more flexible approach, which AustCyber welcomes working with the NSW Government to assist in the development of so a set of arrangements can be developed that better suit smaller companies. There will also be an opportunity within this effort to align internal and external auditing practices and areas of focus for performance audits.

(ii) The risks involved with outsourcing government information systems

Government information systems, like those of many organisations across the Australian economy, are complex and the technology and services utilised needs to be the best available for the service that is needed by the public. Government, like any organisation and set of organisations, needs to

⁶ <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3>



be able to access the best available technology from both within own services as well as from outside government.

Further, many innovations designed to deal with complex technical challenges are often developed outside government and larger overseas sourced technology companies and as such are ultimately perceived as less risky. Similar to many procurement decisions, continually procuring from the same or similar organisations creates a sourcing risk. Digital technologies and information technology is no different. Indeed, by encouraging innovations from a range of industry players, including innovative smaller companies and SMEs is one way to reduce risk. The level of creativity can be higher with different approaches for working on technical problems. In relation to cyber security, by reducing risk more secure digital networks and offerings are developed, again creating greater digital trust.

AustCyber considers that by adopting the approaches recommended in this submission, including developing the Procurement Sandbox so the NSW Government and sovereign cyber security companies can work together to solve complex security problems, the risks of outsourcing government information systems will be reduced. Further, that risks introduced by technology life cycles expiring before an overall project is delivered would be better managed. This is particularly applicable for major physical infrastructure projects reliant on digital technologies as part of delivery (i.e. all projects being delivered by Government).



About AustCyber

AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

We form a part of:

- the Australian Government's Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda, in sectors of competitive strength and strategic priority to boost innovation and science in Australia. Industry Growth Centres are required under contract with the Government to achieve for their sector:
 - increased R&D coordination and collaboration leading to improved commercialisation outcomes
 - improved management and workforce skills of businesses
 - more businesses, including small and medium enterprises, integrated into global supply chains leading to increased export income
 - a reduction in the cost of business through regulatory reform
 - additional or indirect (spillover) outcomes;
- Australia's 2016 Cyber Security Strategy. It was through the industry consultation and development of this strategy that the concept for AustCyber was first conceived.

Our funding comes from majority Federal Government grants – funding for operations and programs, and for the \$15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber's national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market 'hot spots' around the world.