AustCyber
Australian Cyber Security Growth Network

SUBMISSION

2020 CYBER SECURITY STRATEGY CONSULTATION

DEPARTMENT OF HOME AFFAIRS

NOVEMBER 2019

Introduction

It is crucial the next cyber security strategy successfully builds on the security and prosperity foundations and successes of the current strategy.

Cyber security is different to other human endeavours. As noted by the Australian Government's 2016 Cyber Security Strategy, it is different because of the reach of cyber threats, together with the pace and scale at which they can be iterated on and deployed in the online environment, relative to their physical equivalents.

It is also because cyber threats and their resulting risks are highly contextual. What we think we know today, is likely to have changed by tomorrow – in the nature and sophistication of the threats and risks and how they manifest.

The ways and means to manage the risks are also vastly different dependent on the size and type of organisation. Management of the same or similar set of cyber risks will be different for a large organisation versus a smaller organisation, a small organisation in retail versus a local council or a small organisation in specialised medicine or defence industry or child care or craft spirit distilling, a publicly listed company or private entity, an exporting organisation or a startup. And so on.

Organisational and individual need for products and services as a result is broad, dynamic and rapidly growing. Market trends point to tremendous economic opportunity. Global cyber security product sales are predicted to reach US$124 billion in 2019, up from US$114 billion in 2018[i].

The outlook for cyber security spending in the Indo Pacific region is particularly strong. This presents significant opportunities for the export of Australian cyber security products and services – further increased again when indirect benefits of trust and assurance in supply and value chains are considered.

Cyber and <insert here>

The economy-wide need for cyber security and resilience is what makes the cyber security sector Australia's true horizontal enabler. It is now a sector in its own right but it also underpins the success of every other sector and activity (so, cyber and <insert your sector or activity here>). In other words, every part of the economy, including governments, requires cyber security products and services to manage cyber risk. Likewise, all endeavours require cyber security products and services to grow in a world that is connected and data is everything.

A globally competitive Australian cyber security sector will ultimately underpin the future success of every industry in the national economy. It promotes greater trust in Australia as a safe and desirable place for businesses to pursue digitally driven growth and by providing products and services that assure the cyber resilience of all organisations.

The Australian cyber security sector is small, but quickly growing in maturity and size, with an increasing number of home-grown success stories. Australian cyber security software, hardware and services companies have joined global value chains and are establishing a worldwide reputation for high quality, deep tech, niche solutions for increasingly complex cyber risks in a highly contextual, hostile cyber-physical environment.

AustCyber is proud to have played a significant role in the growth and improved maturity of Australia's cyber security industry and broader innovation ecosystem, now alive with a range of startups, scale-ups and mature companies across capability types. At just under three years old, we have proven that a publicly funded, non profit organisation is the right mechanism to coordinate and drive industry growth, that delivers potentially enormous benefits to the economy and to the development of sovereign capability for the nation's security.

A targeted and consolidated effort is needed – and needed now – to continue to build on early successes and sustain Australia's competitiveness and strategic advantages in the creation and commercialisation of cyber security products and services.

There has been and still is a window of opportunity, but it is narrowing as other countries become more coordinated in their sovereign capability development efforts and the impacts of sustained global economic and geopolitical disruption continues to sharpen.

AustCyber's Cyber Security Sector Competitiveness Plan (SCP) and its updates, together with our Cyber Security Industry Roadmap, co-authored with CSIRO Futures and Data61, identify the key issues that the sector faces together with actions that are needed to remove barriers for growth and enhance our global competitive advantages. The reports also highlight the role that cyber security plays as a horizontal sector in enabling growth opportunities in other priority sectors and underlines the importance of greater coordination by government, industry and education institutions to effectively benefit broader Australian innovation and technology uptake.

Through a lens of cyber innovation, the SCP describes goals for Australia's cyber security sector:

- Grow a vibrant and globally competitive sector
- Export Australian capability to the world
- Australia is the leading centre for cyber security education.

Achieving these goals supports the achievement of the nation's broader economic and social goals as well as those of the national security apparatus. Cyber innovation underpins the achievement of the nation's interests and will only become more important and prominent as more organisations 'go digital' and 'go global'.

This submission provides AustCyber's response to the Department of Home Affairs' discussion paper as part of the development of a 2020 Cyber Security Strategy. It groups the discussion paper's questions into several themes:

- The cyber scene: broaden and deepen the picture
- Research and innovation: the engines of strategic benefit
- Australian capability: world leading and growing
- Regulatory evolution: opportunities for sustained success
- Leadership and coordination: #gameon
- AustCyber: our nation's not so secret weapon.

This submission also represents the views of dozens of Australian cyber security companies and as well as Australian and global buyers of, and investors in, cyber security capability and stakeholders within the education sectors, non profits, Industry Growth Centres and the research community. Many have provided their own separate submissions in addition to the views and experiences shared with AustCyber, which have been reflected in this document.

Summary of recommendations

The cyber scene

1. Ensure Government information sharing and reporting (including data released publicly from Joint Cyber Security Centres) continues to evolve in detail and sophistication across multiple contexts, including consideration of data sets on occurrences of cyber threat be broken down into States/ Territories and, for highly prevalent threats, geographically clustered instances as well as locations persistently targeted
2. Guidance should be developed in support of releases of the Information Security Manual (ISM), tailored to organisational type, size and sector to ensure clarity and consistency across multiple contexts – this could be delivered through a framework and business model like that of the FS-ISAC, tailored to Australian sectoral needs
3. Cyber threat reporting should be enriched by including the insights and analysis of Australian and Australian born technology, cyber security companies and researchers

Research and innovation

4. Build on the current strategy's articulation of the importance of research and innovation, with increased focus on the role these endeavours have on the leadership, policy and operational aspects of cyber security
5. Achieve appropriate recognition for cyber security in the Australian and New Zealand Standard Research Classification and the Australian and New Zealand Standard Industrial Classification
6. Describe and invest in national cyber security sectoral knowledge infrastructure through AustCyber to drive increased maturity in the country's cyber security research and innovation, and have a multiplier effect on the value and impacts of outcomes to the country

Australian capability

7. Prioritise cyber security as an area for preferential procurement in governments, leveraging the Proof of Concept Sandbox identified at page 14, part of the sectoral knowledge infrastructure
8. Consider a one per cent requirement in procurements associated with obligations under the Australian Signals Directorate's Essential Eight strategies to mitigate cyber security incidents, and a target of five per cent with a commitment to grow this year on year
9. Provide incentives and leverage methods to encourage organisations across the economy to buy Australian first where possible
10. Preference local companies to write Government tenders for cyber security capability and put in place multi-party writing teams where project complexity requires/ would benefit from multinational experience
11. A whole of Government approach to changing procurement rules is required, also to recognise the horizontal nature of cyber security
12. Lead on the delivery of a platform for a trusted marketplace for procurement within the Five Eyes community, that also supports information sharing on use case experiences of early stage technology
13. Develop incentives that encourage investment in nurturing and supporting sovereign capability for export global value chains; investment in earlier stage technology will create a circumstance for evolving technology to become world class
14. Establish a publicly funded cyber security investment function, through AustCyber

15. Identify the United States' National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework's utility as a standard for skilling and workforce development as well as the benefits of it providing a baseline for skills mobility

16. Consider what more Government can do to speed up the coordinated achievement of quality throughput of students from TAFEs and universities into cyber security jobs nationally (page 22)

17. Ensure the trust model underpinning CISO Lens is accessible to public sector Chief Information Security Officers, Chief Security Officers and equivalent positions in Government and encourage participation from the other levels of Australian government

18. Make short courses or 'bootcamps' for parliamentarians on the technical and non technical threats, risks and opportunities of cyber security mandatory and partner with Australian cyber security companies to develop content

19. Support the development of a baseline curriculum for briefing senior executives and leadership teams, including boards, on broad technical and non technical threats, risks and opportunities as well as additive modules of information for contextual learning across sectors. Consider development of an adapted version of such briefings for educators across Australia's formal education system

20. Describe the key benefits of cyber security skills challenges, competitions and conferences in the development and sustainment of cyber security skilling and Government's role in supporting the scaling of key existing multi-party initiatives

21. Provide the right incentives for a locally developed but globally connected program for commercially accessible, nationally consistent and university recognised training for highly technical operational circumstances, a gap in Australia's current cyber security training environment

Regulatory evolution

22. Undertake a wide ranging assessment of the cyber security implications of Australia's legislative and regulatory frameworks and regimes, across its levels of government; and the implications of Australia's legislative and regulatory frameworks and regimes on the cyber security industry. This should also consider the relative and comparative behavioural impacts of the Notifiable Data Breaches Scheme and *Security of Critical Infrastructure Act 2018 (Cth)* to understand where more could be done to reach affected organisations not yet mature in managing their obligations

23. Provide for reform on the underpinning processes for the development of all legislation and regulations to take better account of both the economic and national security considerations of cyber security

24. Adopt the recommendations made by Standards Australia in their submission to the consultation process and apply a principle of harmonization between government developed and industry generated practice guidance

25. Consider the formal feedback loops that could be formed between Government and industry, perhaps through the partnership between Standards Australia and AustCyber, on current and emerging regulatory matters discussed in the Council of Australian Governments and related fora as well as multilateral fora

Leadership and coordination

26. Return the position of a Minister for Cyber Security to the Ministry of the Parliament of Australia

27. Reinforce the leadership roles in and out of Government that work in partnership to deliver on the mutually beneficial 'protect' and 'grow' missions for cyber security; clarify the roles of

Ministers and pubic officials in Government to remove confusion around changes made in the last year

28. Where appropriate, consider publishing information shared between parliamentary committees and inquiries regarding cyber security

29. Improve the business model, operating principles and coordination of the Joint Cyber Security Centres (JCSCs) and the delivery of activities within them

AustCyber: our nation's not so secret weapon

30. State the uniqueness of AustCyber and it being an asset in supporting the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhancing Australia's future economic growth in a digitally enabled global economy as well as improving the sovereign cyber capabilities available in defence of the nation

31. Note that AustCyber is a critical point of coordination for industry creation and sustainment, forming a key part of the nation's approach to better managing cyber risk and supporting the economy to become cyber resilient

The cyber scene: broaden and deepen the picture

Reflections on the Discussion Paper's questions 1 and 5

The increased complexity of the cyber threat environment is globally recognised. This is in part due to the responsiveness and resourcefulness of malicious actors taking advantage of unsecured rapid digitalization, as well as legacy in ICT infrastructure and human behaviours, human and technological capability gaps. This combined with improving but comparatively still low awareness in broader society, outdated and siloed legislation and regulation, rapidly evolving geopolitical and cultural dynamics and human bandwidth overload – it is more than complex, it is a perfect storm.

It is also due to the asymmetric nature of attacks for small organisations, which comprise 97 per cent of the Australian economy. In a study done by KPMG and then Fairfax in 2018, it was found that around 60 per cent of Australian mid sized companies that suffered a compromise were going out of business within six months[ii].

Since *Australia's Cyber Security Strategy* was released in 2016, there has been an impressive increase in the level and quality of data available on the upside and downside impacts of digital technologies and associated cyber security to Australia's way of life, economy and national interests. Prior to this, data was often regional or extrapolations of global trends.

We commend the Australian Government for providing increased reporting on cyber threats to and incidents in Australia. The improved frequency and depth of information focusing on cyber risk is also encouraging, including through the important work of the Office of the Australian Information Commissioner and the Office of the eSafety Commissioner.

It will be increasingly important to ensure Government information sharing and reporting (including data released publicly from Joint Cyber Security Centres) continues to evolve in detail and sophistication across multiple contexts.

We encourage consideration of data sets on occurrences of cyber threat be broken down into States/ Territories and, for highly prevalent threats, geographically clustered instances as well as locations persistently targeted. This reporting would:

- support the general awareness and understanding by individuals and organisations
- provide trust and certainty for organisational planning, resourcing, strategy and risk management, as well as benefit incident response and management
- provide real-time visibility and guidance to organisations that operate in or supply to critical infrastructure
- improve outcomes from programs initiated by governments in response to specific threats, for example, the MSP3 Program for Managed Service Providers against the so-called Cloud Hopper campaign of global attacks.
- assist local law enforcement and social support agencies better effect their work and identify knowledge gaps.

Of increasing importance, this will also benefit innovators and investors responding to market needs, generated by shifts in legitimate and illegitimate behaviour as well as societal and technological capability gaps.

Further, we recommend that guidance be developed in support of releases of the Information Security Manual (ISM), tailored to organisational type, size and sector to ensure clarity and consistency across multiple contexts. As the economy continues to mature its implementation of cyber security strategies – and malicious actors continue to improve their deployment of attacks – this will likely help organisations more quickly action relevant adjustments in business management and operational practices.

There is an opportunity to partner with the private sector on this, including through Joint Cyber Security Centres (the ‘Australian capability’ section below refers).

Sources of threat intelligence

Australia continues to enjoy increased focus and localisation of data and analysis from globally respected technology companies including Blackberry/ Cylance, Cisco, FireEye, Microsoft, Symantec, Verizon and many others; as well as the major professional services firms including Accenture, BDO, Deloitte, EY, KPMG and PwC and many others; and the critical importance of global and multilateral think tanks and organisations such as the Organisation for Economic Co-operation and Development (OECD) and World Economic Forum (WEF) that advocate sharing of solutions to solve technology based problems.

Broad use of cyber threat information needs to also be enriched by transparently and repeatedly applying the insights and analysis of Australian and Australian born technology, cyber security companies and researchers generating often globally unique data sets.

Equally important are the emerging issues being covered by Australian companies and researchers, as the world grapples with the horizontal nature of cyber threats and their role in common challenges such as deep fakes and electoral interference.

Publicly available examples include:

- Bugcrowd – Priority One Report 2019: The State of Crowdsourced Security[iii]
- Dtex Systems – 2019 Insider Threat Intelligence Report[iv]
- Kasada – Bots Down Under: An Australian Market Threat Report 2019[v]
- Nuix – Discover/ Investigate platforms supporting continuous big data analysis, including the International Consortium of Investigative Journalists disclosures known as the Panama Papers[vi]
- Telstra – Security Report 2019[vii].

Research and innovation: the engines of strategic benefit

Reflections on the Discussion Paper's question 26

As a horizontal enabler, cyber security has a significant role in:

- the creation of globally competitive new industries, including those that flow from significant investments in areas such as defence industry, space capability and advanced manufacturing
- the use of data for innovation and growth
- supporting the economy to push into alternative asset classes
- underpinning trust in the:
    - systems and structures supporting intangible assets to be formally recognised in economic and fiscal policy
    - implementation of new regimes such as consumer data rights and open banking
    - transition to hybrid cyber-physical and new technology environments created by step-change infrastructure such as 5G and quantum.

The role of cyber security research and innovation is not only crucial economically – they are strategic and social imperatives.

The same policy backdrop that established AustCyber also paved the way for boosting the role of Data61 and the Defence Science and Technology Group in the pursuit of world-leading cyber research and innovation, together with funding for the industry-led Cyber Security Cooperative Research Centre, as well as a series of other actions at all levels of government in Australia on cyber industry development and commercialisation.

More effort is needed to capitalise on, as well as scale and embed the contributions made through these investments. As noted above, there is a narrowing window of opportunity to strengthen the nation's competitive advantages in cyber security capability development and commercialisation for the benefit of the defensive mission (applied sovereign capability) and the economy (scaled cyber resilience and export revenues).

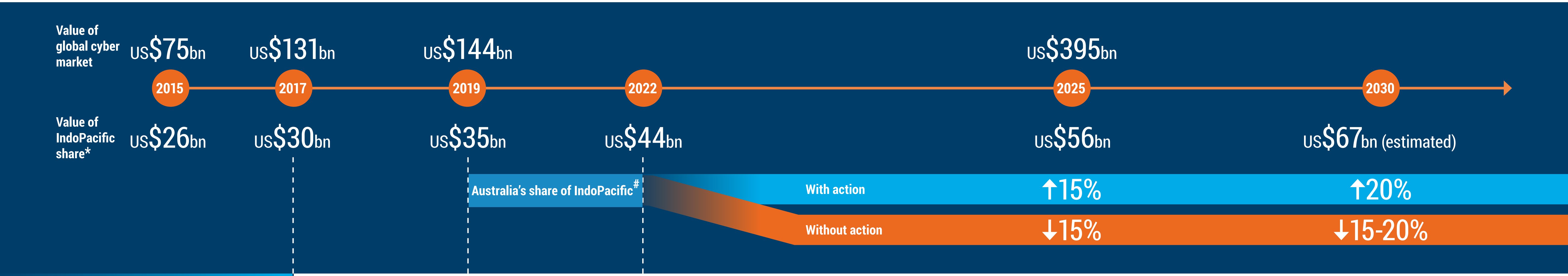
There is also an increasingly urgent need to resolve how best to achieve a 'secure by design' approach to goods and services, including the proliferation of IoT devices, as described in Cyber Security Industry Roadmap, for consumers but also to assure trust in the economy overall.

Over page is a snapshot of this window of opportunity, narrowing because of the convergence of rapid advancement in transformational technologies (including automation) and their supporting business models with cyclical economic disruption and geopolitical pressures.

The 2020 Cyber Security Strategy needs to build on the current strategy's articulation of the importance of research and innovation, with increased focus on the role these endeavours have on the leadership, policy and operational aspects of cyber security.

These are key signals to the market and helps support how the market responds to problems and challenges. It is also key to the success of many of the Government's other policy pursuits, including in other complementary and strategically aligned areas of research and investment in innovation.

Australia's cyber security challenge: Invest and take action now, so we don't fall behind



	2015	2017	2019	2022	2025	2030
Value of global cyber market	US$75bn	US$131bn	US$144bn		US$395bn	
Value of IndoPacific share*	US$26bn	US$30bn	US$35bn	US$44bn	US$56bn	US$67bn (estimated)

Australia's share of IndoPacific#

	2025	2030
With action	↑15%	↑20%
Without action	↓15%	↓15-20%

Sector focus

- Jobs
- Revenue
- Contribution to GDP/GVA

1 Grow both the sector and value of the sector to economy

2 Australia contributing to the global economy

3 Position Australia globally as a cyber innovator

Taking a nationally coordinated approach to driving science, technology and innovation through focused R&D and commercialisation

💰🔒 **Low awareness** in business and community

💰 **Highly fragmented set of stakeholders** across the economy

💰🔒 Increased activity of **nation state actors**

💰🔒 Turbulent **geopolitical environment**
↑ Alliances
↑ Defence
↑ Economic risk

💰🔒 **Somewhat fragmented set of stakeholders** across security apparatus

💰 **Horizontal growth** across sectors improving but inconsistent

💰 Increasing levels of sector focused **legislation and regulation**

💰 Increasing importance of cyber's role in **digital skilling**

💰 Embedded workforce development **framework**

🔒 Increasing sophistication in **criminal and other attacks**

🔒 Increased focus on **5G**

National interest:
🔒 Security 💰 Economy

Burning platform to take action now, requires continuous improvement and collaboration.

Challenges and opportunities

Economy

- Government and large business as consumer
- SMEs vs large / public vs private as producer
- Unifying the federated model on policy and settings
- Preferred procurement of Australian made capability

- Incentivising positive behaviour – as business risk not cyber IT risk
- Incentivising positive behaviour on cyber as growth enabler across all sectors and asset classes
- Emerging new models for measuring cyber growth and applied across sectors

Regulation and policy

- National alignment, view to offshore
- Interoperability and obligations
- Lead in the region
- NICE Workforce Framework adoption
- Dual use capabilities eg. defence industry, space, advanced manufacturing

- Opportunity cost of lack of clarity; impacts:
  - Competitiveness
  - Reputation of Australia in IndoPacific region
  - Profitability and therefore jobs growth
- Telecommunications and other Legislative Amendment (TOLA)
- Other sectors' regulation intersecting with cyber, especially in governance, risk and compliance services

Sector infrastructure

- Driving sector standards
- Developing a trusted marketplace
- Achieving global competitiveness, consistent across key capabilities
- Deepening sovereign capability
- Cross-cutting all sectors

- R&D incubation, commercialisation and acceleration
- Addressing the commercialisation 'valley of death'
- Investment and venture capital funding
- Normalised export pathways
- Data to measure impact and contribution

* IndoPacific figures from SCP. Australian figures not available at present. AustCyber is currently working to obtain them.
# Trend taken from various global indicies e.g. Gross Value Add Index, Global Innovation Index, World Economic Forum reports.

There is also a pressing need to achieve appropriate recognition for cyber security in the Australian and New Zealand Standard Research Classification and the Australian and New Zealand Standard Industrial Classification, which provide the foundational structures for how publicly funded R&D as well as commercialisation is awarded, measured and reported. It also influences the reporting and trend analysis of the transfer of technology and patents.

Not having this achieved is in part why Australia is not yet seeing cyber security feature at scale in research funding rounds. It is also why the sector's research and commercialisation achievements in some capability types are under-reported or absent from assessments of industrial performance.

Ideation to export knowledge infrastructure

The 2020 Cyber Security Strategy can help drive increased maturity in the country's cyber security research and innovation, and have a multiplier effect on the value and impacts of its outcomes, by describing and investing in national sectoral knowledge infrastructure.

The comparative youth of the cyber security sector means its knowledge infrastructure – the value chains, normalised ways and means of doing business and structures to sustain growth and maturity – is still forming and scaling. So too are the mechanisms for meaningful public-private partnerships and repeatable measurement of sectoral value and impact[viii].

As has occurred with the support of sustained Government funding across decades in older sectors of the economy, we consider the development and implementation of such infrastructure, designed to the needs of Australia in the context of both the Indo Pacific and global markets, is needed to capitalise on early growth for a sustained, high value sector that delivers innovative sovereign capability.

We have undertaken research across key international locations for cyber security research and innovation systems, as well as domestically in other sectors, to identify the key elements of sectoral growth from a knowledge infrastructure perspective.

See over page for our resulting conceptual model.

The presence of startup hubs, as well as incubators and focused accelerator programs, are critical components of building and maintaining a vibrant and globally competitive cyber security sector. The United States Department of Homeland Security and SRI International[ix] have published specific insights on the role of knowledge infrastructure in the technology transition period of commercialisation, so companies have a measurably higher rate of success in achieving access to market and growth opportunities.

Trusted vetting of cyber security solutions is also a key factor for sectoral success (achieved in the model through a 'Proof of Concept Sandbox', connected to a Government approved test lab). This underscores the technical veracity and scalability of a product or service. Further, it tests market competitiveness across the different layers of the domestic market and different contexts of international markets. In a sandbox environment, deployment simulations support better solutions integration, legacy implications and enhance benefits realisation from onboarding and sustaining new/ different technologies.

Further, a well-informed investor community that appreciates the different needs for scaling cyber security products and services – that is, confidence in the deployment of both patient and rapid capital across numerous capability types and contexts – and how to navigate global regulatory challenges is equally key to sustained scaling and growth.

Importantly, thought has been given to the merits of this infrastructure to delivering a trusted marketplace with skilled professionals and providing a valuation of the sector's significant intangible assets.

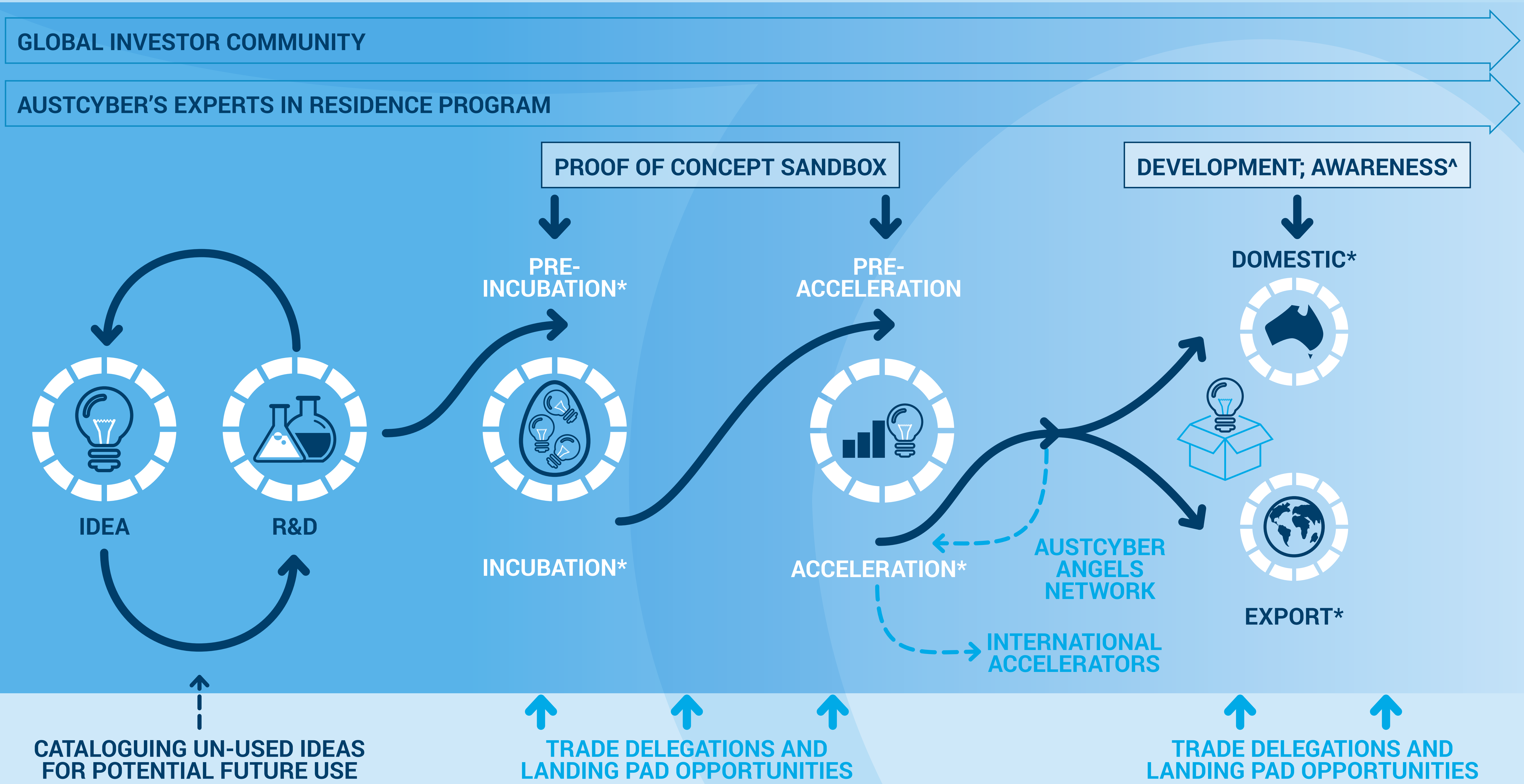
Australian Government
Department of Industry, Innovation and Science
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network

Australia's cyber security sector: Build local, deliver global

Ideation to export infrastructure

Supported by AustCyber's network of innovation nodes and challenges platform



GLOBAL INVESTOR COMMUNITY

AUSTCYBER'S EXPERTS IN RESIDENCE PROGRAM

PROOF OF CONCEPT SANDBOX

DEVELOPMENT; AWARENESS^

IDEA

R&D

PRE-INCUBATION*

INCUBATION*

PRE-ACCELERATION

ACCELERATION*

AUSTCYBER ANGELS NETWORK

INTERNATIONAL ACCELERATORS

DOMESTIC*

EXPORT*

CATALOGUING UN-USED IDEAS FOR POTENTIAL FUTURE USE

TRADE DELEGATIONS AND LANDING PAD OPPORTUNITIES

TRADE DELEGATIONS AND LANDING PAD OPPORTUNITIES

* = Exit (merger/acquisition) possible at any of these stages

^ = Manager talent development; Investor & buyer awareness

The model considers how to flexibly provide for product/ service innovation, alongside investment, business acumen and talent pipelines for workers, entrepreneurs and innovators (suppliers) and executives/managers (buyers and investors in public and private sector settings). It also considers impacts of step-change interventions, from within the sector (through technological advancement or policy/ regulatory change), or from external sources such as disruptive business models or human behavioural change.

The infrastructure should preference Australian cyber security companies but not be exclusive to them, leveraging the partnerships between AustCyber, Austrade and industry in achieving strength in a competitive domestic market that includes expanding cyber security to consider its impact on AI, robotics, space and qantum, for example.

The infrastructure will be flexible in its systems and processes such that an individual/ organisation will be able to access any stage in the model. Should an organisation wish to enter at the incubation stage or beyond, their entrepreneurial and solutions readiness will be assessed for appropriateness.

Each stage will also leverage other flagship programs and initiatives, in particular AustCyber's national network of Cyber Security Innovation Nodes, operated in partnership with State and Territory governments, and the network's counterparts in other growth sectors[x], and the Government's national network of Joint Cyber Security Centres.

National Cyber Security Ideation to Export Infrastructure will provide the foundations for the long-term successful growth of a vibrant Australian cyber security sector by:

- deliberately and strategically supporting the growth in the number of Australian cyber security companies.
- identifying and providing targeted support to potential high value, high impact cyber security companies.
- providing a comprehensive approach to sustained ecosystem growth and strategic outreach to buyers in other sectors.
- linking to talent and solutions development opportunities in key international markets.
- positioning Australia as a visible and highly competitive producer of cyber security companies and innovative solutions, including services such as governance/ risk/ compliance and education where Australia has particular market advantages.
- incentivising systemized feedback loops on employer needs from formal education offerings.
- generating opportunities for individuals, startups and scale-ups to develop, test and market ideas that solve Australian and global cyber security problems.
- providing formal and informal entrepreneurial, investor and buyer awareness and education which in turn also informs the pipelines of potential cyber security workers.

State of play for the infrastructure build

AustCyber's SCP and Industry Roadmap have provided uplift on the data and context needed to guide the development of the knowledge infrastructure. The SCP is now one of the world's most cited documents on cyber innovation and cyber sectoral growth, with its analysis of capability competitiveness and data on skills and workforce development the most trusted source of such information in Australia[xi]. Its Knowledge Priorities are a leading source of guidance for universities and researchers, also forming an integral part of the research programs of Data61 and the Cyber Security CRC.

A range of other sources have been collated to inform the infrastructure build with further sources no doubt available.

AustCyber's growing national network of Cyber Security Innovation Nodes, co-funded and managed with State and Territory governments, provides a set of networked starting points for the knowledge infrastructure to be delivered through. A number of other sites/ locations have been identified, as well as gaps including in regional and remote Australia, will to be considered and addressed as part of AustCyber's partnerships with State and Territory governments and others.

On the specific stages of the knowledge infrastructure model, at a national level there are some elements already in operation. This includes:

- Ideation
    - Most Australian governments are investing in small scale programs in stage, through their innovation and in some cases skills/ education programs. A small number of industry and community based organisations also convene activities. Two promising examples of ideation oriented programs:
        - the multi-location bootcamps provided by CyRise, Australia's only cyber security specific accelerator, supported by a grant from the Government's Incubator Support Initiative
        - the Canberra Innovation Network's cyber security specific rapid ideas pitch events convened in conjunction with AustCyber's Canberra Innovation Node.
- Research and development
    - This stage is the most mature in the model's life cycle but is not yet deliberately or strategically connected to the stages either side.
    - The Australian Government has invested $50 million over seven years in the Cyber Security CRC. There were security related commercialised outcomes from the completed Data to Decisions CRC. Data61 and the Defence Science and Technology Group have mature, deep technology research programs. All are connected in some way internationally.
    - Most Australian universities have in place or are building cyber security R&D programs, some of which are connected to stages either side and have partnerships internationally.
    - The majority of Australian cyber security companies are currently undertaking some form of R&D for innovation and commercialisation purposes, a small number supported by AustCyber's Projects Fund. A growing number of larger companies are also undertaking some form of R&D and/or innovation that is cyber security related.
- Pre-acceleration/ acceleration
    - CyRise is maturing its business accelerator program including through strategic partnerships with organisations like AustCyber, the Australian Cyber Security Centre, the Australian Information Security Association and connections internationally.
    - Stone+Chalk is providing a business accelerator program that includes cyber security as a key area for the South Australian government in LotFourteen.
- Knowledge for sustained innovation and iteration
    - There are strong elements in place across the country, which provide connections between the infrastructure's stages to retain as much intellectual value in the

economy as possible, that would benefit from scaling and measuring. Examples include cyber security skills challenges and hackathons (next section refers) and AustCyber's AllStars program, which brings non cyber expertise to the sector for knowledge uplift and takes cyber security expertise to the economy.

Most of the stages of the knowledge infrastructure, however, are largely being serviced by localised, sub-scale and fragmented activities – reflective of the sector's age and maturity. A more comprehensive study is needed to provide a map of what is in play, how they are connected to each other and their readiness to be plugged into a more coordinated and nationally.

AustCyber is well placed to be the coordinating partner of choice for Government to invest with key government and industry stakeholders in this formative national infrastructure and extract maximum economic value for sectoral growth. This would cement the country's ability to be more self reliant in pursuit of its security interests.

Australian capability: world leading and growing

Reflections on the Discussion Paper's questions 9, 12, 13, 14, 21, 23

The year on year growth in the global and domestic cyber security markets and the policy settings already described have given rise to a fast growing ecosystem of cyber security startups, and an increasing number of early stage companies on the verge of scaling. There are now more than 300 companies in AustCyber's portfolio; the number has almost doubled each year since AustCyber commenced.

Additionally, Australia offers an ideal growth environment for cyber businesses, due to strengths in core research areas like quantum computation, wireless technology, trustworthy systems and niche high-value hardware. Further draw cards include Australia's large services economy, education system, sound governance settings, economic stability and high living standards. The proximity to the fast-growing and increasingly digitised Indo Pacific region also adds to our natural advantages.

These existing strengths put Australia in a favourable position to develop a vibrant and globally competitive cyber security sector. This gives the double benefit of jobs and revenue growth, with the servicing of sovereign cyber security capability needs. Economic analysis in the SCP shows the sector has the potential to almost triple in size in coming years, with projected revenue soaring from just over A$2 billion in 2016 to A$6 billion by 2026.

Australian cyber security companies are now reporting additional flow-on effects in concurrent industries. This will likely see the broader contribution of cyber security to the economy deliver much more than A$6 billion.

As it was put to AustCyber by one of the sector's fastest growing companies, "the tipping points are stacking up; we would not have talked about manufacturing in cyber a couple of years ago, but we are now. The industry has professionalised – people and businesses that otherwise would have never expanded are going global in meaningful ways. It will several more years to see the full return on investments in the technologies but increased revenue and jobs growth is already strong."

AustCyber's projections of the potential size of prize for the sector and, by association, the economy is laid out over page. The window of opportunity described earlier has enormous potential benefits. But a double negative of reducing trust and capacity in other sectors of the economy if we miss the opportunity to capitalize on growing consumer interest, the investments made so far and pull through benefits for risk management in supply chains.

In the immediate term, there are three reoccurring challenges raised with AustCyber by Australian cyber security companies, regardless of size and business maturity, preventing more rapid and sustained growth in those figures:

- procurement procedures and practices of governments and larger companies
- lack of access to sovereign/ appropriate sophisticated risk capital
- lack of access to skilled people.

The 2020 Cyber Security Strategy and other policy provides a key opportunity to tackle these challenges, described below.

Australian Government
Department of Industry, Innovation and Science
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network

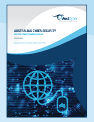
AustCyber's role in sector growth:
Invest and take action now, so we don't fall behind

Global cyber market

2015	2017	2019	2020	2022	2025	2030
US$75bn	US$131bn	US$144bn			US$395bn	~8% annual growth globally

- **Australia's Cyber Security Strategy (current)**
- **Establishment of AustCyber**
- **New cyber security strategy**
- **End of current funding**

AustCyber achievements and deliverables


Australia's Cyber Security Sector Competitiveness Plan (SCP)

Australia's Cyber Security Industry Roadmap

Network of Nodes

TAFECyber

CyberTaipan

Projects Fund

AustCyber OKRs

- Capability map
- Cyber business toolkit for growth success
- International Network of Nodes
- Domestic innovation superclusters
- Ideation to export knowledge infrastructure
- Activating investor community
- Implementation of NICE Workforce Framework into governments and businesses; embedded into education system

- **Objective 1:** Scaled cyber security innovation superclusters, supported by a national network of nodes
- **Objective 2:** Sector knowledge infrastructure supporting commercialisation and innovation
- **Objective 3:** Robust export pathways to key markets
- **Objective 4:** National platform for cyber security skills development and workforce growth

Australian cyber ecosystem

~150 companies

300+ companies

500+ companies

800+ companies

1,000+ companies

Sector conditions

- Not a recognised sector
- Low export activity and poor means of economic measurement
- Lack of knowledge and infrastructure to support growth

- Recognition of sector as a horizontal
- Growing national coordination
- Raised international profile (UK, USA, ASEAN)
- Seat at the table on policy e.g. TOLA, Cyber Security Strategy 2020

- Advent of emerging technologies
- Changing workforce
- Unpredictable and volatile geopolitics
- Structural upheaval driving intersection of economy and national security
- Lack of metrics and data

- **1st unicorn**
- Australia recognised as lead in cyber APAC and global
- Strong International investments from desired sources
- Active venture capital community

- At least 18,000 new workers in cyber security across economy (SCP)
- Increased economic value to sector due to sophisticated and mature infrastructure

- **10+ unicorns**
- Normalised sector treatment and recognised as key enabler of growth of all sectors in the ecomomy

Next steps:

1. Expand AustCyber's remit and role, consistent with industry and national security polices
2. Increased funding to invest in sectoral infrastructure, coordinated by AustCyber (with DIIS and ISA)
3. Improve positioning and gravitas to increase impact on legislation, regulation and sector growth
4. Address structural opportunity in Innovation/Science and Technology infrastructure
5. Align Government funding and program support to the economic potential
6. Develop sophisticated strategy through enhanced measurement and data

Opportunities to double down on AustCyber's role and success so far

- Cyber Security Strategy 2020 (Home Affairs)
- Digital and cyber jobs package (Jobs and Small Business)
- Science and technology prioritisation including Government, emerging technologies, recognising cyber's enabling/horizontal role
- Consistency of approaches to cyber security funding in States and Territories
- Global negotiations on AustCyber equivalent starting with New Zealand and United Kingdom

Changing procurement practices changes the game

Now there is proven growth in a globally competitive Australian cyber security sector, there is enough depth of activity to follow through on prioritising the industry creation side (supply) and start preferencing local industry where possible in government (demand) to see the industry scale and sustain its growth.

While we are seeing some positive results from combined efforts from AustCyber and industry to facilitate Australian capability into contract and related opportunities, it remains sub-scale. The majority of demand continues to come from offshore markets, particularly from industry, defence and government in the United Kingdon and United States. This is good on the export front, but diminishes Australia's credibility as a domestically recognised producer of high tech cyber security capability if its own country does not buy it or back it.

Governments are well positioned to influence the pace and depth of growth, in particular through strong and innovative policies and practices in procurement and onboarding of products and services. This would follow in the footsteps of other areas of capability need in the economy, such as defence industry and space. The prioritisation of cyber security as an area for preferential procurement in governments is well timed and should be supported by the notion of a Proof of Concept Sandbox mentioned above.

It would work to de-risk business maturity aspects of the provider (where relevant and to the extent possible) together with the veracity of the product/ service being sought. It would also likely help mitigate potential risks with the process of Government being the first customer of early stage companies. Further, tt is a significant opportunity to shape and collaborate on use cases across domains/ portfolios and could provide efficiencies in onboarding/ implementation.

Overlaying AustCyber's Projects Fund methodology 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.

The sandbox concept can assist industry to rapidly upskill in supplying to Government, as the majority of the sector's early stage companies are inexperienced in selling to Government as a first customer.

Delivering on a preferential approach would provide leadership across governments and in the economy, while also delivering benefit to Government. A one per cent requirement in procurements associated with obligations under the Australian Signals Directorate's Essential Eight strategies to mitigate cyber security incidents, for example, would unlock tens of millions of dollars in contracting opportunities – a target of five per cent with a commitment to grow this year on year as the industry grows is a game changer.

This would also help set in motion a long term approach to ensuring self reliance in capability development and delivery in critical infrastructure, while not stifling foreign direct investment or multi-party collaboration and innovation.

Comments provided by stakeholders to AustCyber as further considerations for improving approaches to procurement include:

- provide incentives and leverage methods to encourage organisations across the economy to buy Australian first where possible. The United States and Israel do this well.

- preference local companies to write Government tenders for cyber security capability and put in place multi-party writing teams where project complexity requires/ would benefit from multinational experience. Australian cyber security companies have no chance to compete if the specifications are written such that they automatically discount smaller and medium sized companies to tender. Scoping and Requests for Tender should be based on requirements and problem statements, not vendor features.

- the Digital Transformation Agency’s Digital Marketplace is not being utilised effectively for cyber security, with many agencies having exemption and/or going outside the remit. Anecdotal evidence indicates that where Australian cyber security companies have been successful in selling to Government, it has been outside of the Marketplace process. A whole of Government approach to changing procurement rules is required, also to recognise the horizontal nature of cyber security.

- build a platform for a trusted marketplace for procurement within the Five Eyes community, that also supports information sharing on use case experiences of early stage technology.

- develop incentives that encourage investment in nurturing and supporting sovereign capability for export global value chains. Investment in earlier stage technology will create a circumstance for evolving technology to become world class.

Investment and capital to seed cyber security capability growth

Lack of sophisticated risk capital to support the growth of a vibrant innovation ecosystem is a significant barrier faced by Australian cyber security companies, with startups and early stage companies finding access particularly challenging.

While the investment landscape is changing for the sector, venture capital funds, private equity firms and institutional funds remain largely reluctant to invest in early stage cyber security technologies, with the preference to wait until there is evidence of customer and revenue growth, which for some capability types can take much longer to develop in the cyber industry.

As the Australian Investment Council (AIC) have noted in their submission, the opportunity to improve the capacity for the Australian private capital industry to support greater investment into home-grown cyber security and data privacy businesses does exist. We agree with the AIC that boosting the level of investment will serve a dual purpose:

- creating greater access to relevant products and services for consumers to manage key areas of cyber security risk, and

- generating enduring economic benefits for the nation as a whole as those businesses expand into international markets and as part of that, create new employment opportunities for the next generation of Australians.

While Australia has recognised the opportunity to capitalise on the underlying strong footprint we have in the cyber security sector, actual investment in technical capability development and scaling remains a modest amount in the overall mix of venture capital invested in technology and digital sectors. Encouraging the necessary level of private capital investment requires a targeted and strategic focus that is supported through coordinated policy, regulatory and market-based solutions.

According to the AIC, growing the proportion of capital moving into the cyber and privacy areas will be driven by three key factors:

1. Encouraging greater patient capital investment (noted in the ‘Research and innovation’ section above) through fund managers and institutional investors

2. Scaling and coordinating efforts attracting more desirable and focused offshore investment into Australia’s cyber security sector

3. Improving links, knowledge and skills shared between researchers, entrepreneurs and investors (adding further weight to the discussion above on investing in knowledge infrastructure).

AustCyber has been partnering with AIC on two key impediments: improving the level of knowledge and expertise in the cyber security area within the Australian private capital sector, and improving the level of knowledge and engagement between early stage cyber security companies and the established private capital investment sector both here in Australia, and abroad. These are small steps with limited resources. Policies and coordinated legislation that actively focus on the three areas above are needed to truly lift the level of investment into the sector.

The newly formed CyberCX, backed by private equity firm BGH Capital, is the first large scale cyber specific investment that the sector has had to date. The investment brings together 12 of Australia's independent cyber security companies and will provide a ‘one stop shop’ of governance, risk and compliance services[xii]. This type of consolidation at this stage of the sector’s maturity is expected to encourage positive competition and create momentum in the economy, including through the creation of jobs and other direct and indirect flow-on effects.

The growing maturity of the sector through the lens of investment means there will be even greater demand for the right mix of available patient and rapid capital to underpin success in sustained outcomes through the stages of ‘ideation to export’. The CyberCX example is one of many indicators of this increased need but also opportunity.

We recommend the Government consider the potentially considerable benefits of being an active participant in this by establishing its own cyber security investment function, through AustCyber, which could be modelled on the UK Government’s National Security Strategic Investment Fund, operated by the government owned British Business Bank. The fund should be of significant size and leveraging the Knowledge Priorities in the SCP, as well as capability development objectives of Data61, Defence Science and Technology Group, the Cyber Security CRC and the cyber security implications of Knowledge Priorities of the other Growth Centre SCPs.

AustCyber as the delivery mechanism removed the need for a new entity to be established and leverages the already existing and proven Projects Fund framework. This would serve as an entry point at seed stage and remain as grants to prove technical veracity and market scalability. The more significant follow-on investments would be awarded to the high potential, high value projects that could be co-funded by other appropriate industry investors (such as institutional funds). It would learn from and complement other ‘like’ mechanisms such as Main Sequence but be specifically and wholly focused on cyber security and its multiplier effects across the economy, with only sovereign co-funding where co-funding was deemed appropriate.

Discussion on this recommendation has been initiated directly with the Minister for Industry, Science and Technology together with the Department of Industry, Science and Technology. AustCyber would welcome the opportunity to brief the Department of Home Affairs on this as part of finalising the 2020 Cyber Security Strategy.

Sharing the load, improving scale and reach

Incumbent business models need disruption if organisations are to keep pace with accelerating technology change and remain competitive. Common problems of cultural resistance, legacy architectures, over-emphasis on inflexible platforms and ill-suited governance processes have proved difficult to overcome for most large incumbent organisations in the traditional sectors of the economy. The mobilisation of processes and people to address key risks is a key area that these businesses can use to improve their cyber resilience and improve their digital posture.

As documented in several cross sectoral studies, including through a State of Play survey of Australia’s mining and resources sectors, co-funded by AustCyber and METS Ignited, Australia’s Mining Equipment, Technology and Services Growth Centre, the category of risk that remains is about legacy. A large number of core operational technology systems, particularly in critical infrastructure, are married to extremely out-dated applications. This is as true for the space and airline industries as it is for mining.

Complexity is becoming unmanageable as such legacy systems become intertwined with technologies due to the sheer rate of adoption, both planned and unplanned. The purchase of cyber security solutions alone is not the answer. These organisations and sectors need more direction,

guidance and incentives to fundamentally change the way that they operate and in doing so, help to secure the Australian economy.

Noted in the ‘The cyber scene’ section above is an opportunity for Government to work with a trusted partner to undertake the provision of public guidance supporting the releases of the Information Security Manual, tailored to organisational type and sector to ensure clarity and consistency across multiple contexts. Further, there is opportunity for a non profit, experienced organisation to better undertake the preventative/ proactive activities of the Joint Cyber Security Centres (such as educational security briefings, exercising, information and data sharing) with higher frequency and specificity.

A framework and business model like that of the FS-ISAC, tailored to Australian sectoral needs, could respond to the above opportunities – and provide better enablement of threatcasting and systemic problem solving that involves smaller, innovative Australian cyber security companies as well as smaller companies in other sectors, who currently are largely unable to access Joint Cyber Security Centres at present. It would also allow for more rapid interconnectivity with trusted global information networks and, over time, industry-led capacity building and a likely new form of market access for export opportunities.

Australia as the leading centre for cyber security education → Skilled people supporting trusted markets

We welcome the clear focus from Government on the need for a globally competitive national cyber security workforce and how critical this is to economic prosperity and national security; the severe shortage of job-ready workers is a key operational challenge but also a barrier to sectoral growth.

Latest data in the SCP and through AustCyber’s regular engagement with cyber education providers indicates that Australia’s cyber security workforce is growing strongly, but not sufficiently to fill the substantial short-term demand for cyber security professionals.

The core cyber workforce has increased by seven per cent to around 19,500 workers over the past two years. This growth is mostly driven by workers transitioning from adjacent sectors such as IT. Graduates and skilled migration – the two other key sources of supply – have so far contributed relatively little to Australia’s cyber security workforce growth (noting there is a natural lag in growing the number of graduates from the time of successfully improving enrolments).

Measuring the precise size of a skills shortage is difficult because of the dynamic nature of labour markets. Calculations using a range of methodologies, based on a combination of the job market indicators, suggest Australia’s cyber security sector was short 800 to 2,300 workers in 2017. That is equivalent to roughly four to 12 per cent of the total Australian cyber workforce in that year.

The workforce shortfall has significant economic consequences. The cyber security sector is estimated to have forfeited up to $405 million in revenue and wages in 2017, which it could have generated if companies had been able to find the cyber security workers to fill existing vacancies.

The SCP details strategic actions for all actors in the sector to deliver on the goal of making Australia a leading centre for cyber security education by:

- Attracting the best and brightest to cyber security
- Ramping up multidisciplinary technical and non technical cyber security education and training
- Creating vibrant, industry-led professional development pathways.

Working with the private and public sectors and the academic community, AustCyber has made significant strides in addressing workforce challenges, including through AustCyber's Project Fund, which to date has co-funded:

- the University of Sydney's Australian Computer Academy, in partnership with ANZ Bank, Commonwealth Bank of Australia, National Australia Bank, Westpac Banking Corporation and British Telecom, to develop and implement Schools Cyber Security Challenges for high school students, that provide nationally consistent in-class cyber security skills packages embedded the national Digital Technologies curriculum (total project funding of $1,230,435). Over 60,000 students have completed challenges in the first 12 months of the program operating.

- Fifth Domain to produce a learning management system, in partnership with the Canberra Institute of Technology, the Australian National University, and Nova Systems that enables education organisations, students and employers to collaborate in developing the cyber security workforce of the future (total project funding of $1,094,228).

- WithYouWithMe to identify, train and add 75 new students into the Australian cyber security industry as a pilot of their cyber skills development platform (total project funding of $300,000).

Also as part of the SCP actions on workforce development, AustCyber has:

- worked collaboratively with TAFE institutes and industry partners across the country to develop a comprehensive cyber security TAFE curriculum, rolled out in January 2018. We subsequently established the TAFECyber Strategy Working Group to support TAFEs to mature their underpinning delivery systems, work through operational challenges such as teacher skilling and shortages, better coordinate curriculum updates, build and deploy training Security Operations Centres and progress efforts to connect vocational qualifications to high schools and universities

- provided strategic focus to the Department of Education and Training's cross-sector cyber security project through PwC's Skills for Australia, which is developing cyber security competencies for deployment across all vocational education and training packages. The project is expected to be completed this year

- coordinated industry participation in the Australian Government’s recent addition of two more cyber security focused Pathways in Technologies (P-TECH) schools (including VET in Schools), in Victoria and Western Australia. AustCyber has facilitated participation in these two sites, including Australian Computer Society, Australia Post, Asterisk Information Security, Box Hill Institute, BHP Billiton, Diamond Cyber, Forticode, Hivint, Kinetic IT, nbnco, North Metro TAFE, Swinburne University of Technology, Telstra and University of Melbourne

- in partnership, delivered and supported a series of national and local cyber challenges which encourage growth in the skills pipeline, talent identification and continuous learning. This includes our partnership with Northrop Grumman Australia to deliver a national pilot for youth cyber defence challenges in CyberTaipan, the Australian version of CyberPatriot in the United States and its other sister programs CyberTitans in Canada, CyberCenturion in the United Kingdom and CyberAriabia in Saudi Arabia.

We have also leveraged its Projects Fund framework to put forward a potentially multi-party industry led proposal to the Government’s establishment of a Skills Organisation Pilot in Digital Technologies and Cyber Security under its $525.3 million Skills Package, for the deployment of funding to activities for digital and cyber skilling across Australia.

A high proportion of the applications in AustCyber’s current round of its Projects Fund (which has $8.4 million available for matched funding) are aligned to skills and education sector challenges which may see further investment in projects with national impact for cyber security skilling.

While many of the achievements to date are young and will take time to reach full maturity and scale, they demonstrate high levels of effective collaboration and growing levels of impact.

Much like addressing procurement practices is a next step for a growing supply of cyber security products and services, a next step in workforce development is ensuring the entry level competencies are addressed (schools curricula, employment pathways from school age leavers, retraining mid career for academia or industry etc.) and the commensurately scaled supply of skilled people through to the most highly technical are available.

Many of the achievements noted in this submission have leveraged and/or integrated the globally recognised National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework developed in the United States. Our engagement with larger employers in Australia, public and private sector alike, have seen uptake of our dashboard resources to use the NICE Framework as a consistent baseline for workforce planning and development as well as retention and planned mobility. This has been further enhanced by our membership on the Global Forum for Cybersecurity Expertise's Working Group D: Cyber Security Culture and Skills.

Opportunities for further focus in the talent pipeline

The 2020 Cyber Security Strategy should note the NICE Framework's utility as a standard for skilling and workforce development, as well as the benefits of it providing a baseline for skills mobility (with follow-on benefits for applicable classes of visas and talent exchanges).

Under the current structure of cyber security in Government, it will be critical for the Defence; Employment, Skills, Small and Family Business; Industry, Science and Technology; and Home Affairs portfolios to be involved in the work of the Department of Education and Training, in particular on reviews to the Digital Technologies curriculum. These efforts should seek to significantly expand opportunities for cross sectoral input from industry.

TAFEs and universities also report plans for continued investment in cyber security, including in applied learning environments like training Security Operations Centres, internships and incentives for increasing enrolments. The pull through of Masters and PhD students into the economy will also start to occur, including through the incentives provided by the Cyber Security CRC. State and Territory governments are also contributing – for example, in South Australia, cyber security is a priority for 2,600 government traineeships and in Victoria, the Certificate IV in Cyber Security is on the list of tuition-fee free courses. The Government should also consider what more it can do to speed up the coordinated achievement of quality throughput of students into cyber security jobs nationally.

There is clearly more that needs to be done to help achieve more certainty for students, parents, teachers, employees and employers around careers in cyber security. We welcome the opportunity for our expertise to be further leveraged for scaled, coordinated national benefit in growing efforts to further deepen the talent pipeline and workforce development.

Informed risk decisions gives rise to improved resilience

As the sector matures, there is increased need for specialised aspects of the knowledge infrastructure worth singling out in the context of Australian capability. This includes the critically important role of the Chief Information Security Officer (CISO)/ Chief Security Officer (CSO) and ensuring the people occupying these positions within organisations have trusted networks to rapidly share experiences and have capacity to reflect on what is and what is not working in the operational environment.

This kind of knowledge sharing extends to a sandbox for problem identification, a common challenge in larger organisations, together with developing better practices for the operationalisation of new and innovative products and services. The ultimate outcome over time is more informed risk based decisions in the cyber domain.

The Australian company, CISO Lens, has responded to private sector demand for this kind of function. There is an opportunity to ensure the trust model underpinning CISO Lens is accessible by public sector CISOs and CSOs across levels of government – and for the private sector group of

CISO Lens members to link to a government group of CISO Lens participants to support cross pollination of contextual knowledge and expertise.

Further, CISO Lens facilitates a CIO group and has a CISO/ CSO group operating in New Zealand. Of growing value, the company also publishes an annual benchmark report on the cyber landscape through the eyes of a CISO/ CSO.

Investment from a leadership perspective in this as a knowledge capability for the economy will pay dividends at critical operational moments and in managing trends around burnout[xiii]. It will also help normalise the role of cyber security and managing cyber risk in larger organisations and then in turn through supply chains.

Bootcamps for boards, senior decision makers – and educators

Another gap in cyber security skilling is the scaled access to consistent, trusted learning for decision makers. Short courses or 'bootcamps' for parliamentarians on the technical and non technical threats, risks and opportunities of cyber security should become a mandatory feature of Australia's political landscape as is the case in several of our closest offshore partners. Government should partner with Australian cyber security companies to develop bootcamp content.

A baseline curriculum for briefing boards, senior executives and business leaders, on broad technical and non technical cyber security threats, risks and opportunities should also be developed and regularly updated by independent, accredited experts – as well as additive modules of information for contextual learning across sectors. This would provide national data measuring measure board and executive understanding and tolerance of cyber risk, as well as inform the development of curriculum based on business trends. In addition, this kind f leadership will contribute to setting an effective tone and culture for all Australian businesses.

There is also significant merit in considering an adapted version of such curricular for all educators across Australia's formal education system. If teachers themselves are not cyber aware, then how are they able to lead and influence our children on cyber security risks and consequences? It would highlight the horizontal nature of cyber security as a cross disciplinary application, as well as improve the academic institutions cyber posture, who themselves are subject to malicious attacks. In addition, this will assist teachers in school environments to have informed discussions with parents and students on possible cyber security career options.

Generating the sharpest skills for the highest level of operational complexity

Australia has demonstrated it has the ability and competence to deliver focused and scaled cyber security skills oriented challenges, competitions and conferences.

The gamified format of skills challenges includes technical hands-on keyboard as well as non computer-based competitions. Technical challenges often involve learners demonstrating their ability to protect against would-be attackers or exploit security flaws. Non computer-based challenges can be used to demonstrate a learner's policy, strategy, legal and business acumen to solve real or simulated cyber security problems facing countries and organisations today.

In both types, skills challenges are proven to encourage team work, critical thinking, problem solving, effective communication and other skills and abilities that supplement work role specific skills relevant to jobs within the sector. They also help generate interest in cyber security jobs and careers and provide a means of continuous, life-long learning.

The 2020 Cyber Security Strategy should acknowledge the key benefits of cyber security skills challenges and conferences, in particular when they are measured and trend data of their impacts made available, and suggest Government's role in supporting the scaling and sustainment of key existing multi-party initiatives, such as:

- the Schools Cyber Security Challenges for high school classrooms and CyberTaipan for applying learning from the classroom (noted above) – both have been designed to complement each other and provide an almost unique skills development package, including the ethics and context of cyberspace, that is about to be exported
    - there is opportunity to also adapt the Schools Cyber Security Challenges and CyberTaipan for primary schools, for which there is interest in several jurisdictions
    - it should be noted that analysis in other countries shows the presence of skills competitions across the school year provides a positive outlet for students to apply the skills they are learning in the classroom, in an environment where they are also learning the legal frameworks of cyberspace and consequences of malicious activity (tailored to the year level of learning)
- CySCA – Cyber Security Challenges Australia – for vocational and higher education students
    - AustCyber has provided a separate proposal previously to Government on scaling CySCA, leveraging the program's strong foundations and scalable ICT infrastructure
- BSides, which operates in Canberra (the second largest in the world), Melbourne, Perth and Sydney and other conferences and events such as CrikeyCon, Ruxcon and WACTF
- non technical skills based events such as the Cyber 9/12 Strategy Challenge and DFAT's Technology for Development Challenge.

Scaling these activities would complement industry led knowledge growth activities including conferences such as CyberCon, convened by the Australian Information Security Association. There are also discussions within the sector on how to leverage existing upwards trends in skills availability and quality to attract global events like Black Hat and DEFCON to Australia. These would add to a growing presence of RSA Conferences, for which this year AustCyber partnered with the NSW government and RSA Conferences to bring RSA Unplugged to Sydney, the first time an RSA Conferences event has been convened in the Southern Hemisphere.

In terms of having ready access to commercially accessible, nationally consistent and university recognised training for highly technical operational circumstances, a current gap in Australia. Addressing this gap in a repeatable and measurable way will become increasingly important as the impact of sophisticated attacks are felt through supply chains, mobile/ decentralised ICT infrastructure and devices, automation and artificial intelligence and increasingly regulated environments. There is an opportunity for the 2020 Cyber Security Strategy to acknowledge this as part of the maturing process of the sector and its role in the economy and, in doing so, provide the right incentives for a locally developed but globally connected program to emerge.

Attracting an event like DEFCON to Australia and being able to routinely send Australian teams to successfully participate in the global DEFCON competitions (held in Las Vegas annually) would also be a proof point of investment in a scaled, commercially available program for highly technical skills.

Regulatory evolution: opportunities for sustained success

Reflections on the Discussion Paper's questions 5-8, 10-11, 15-19, 21

There have been a growing number of regulatory reforms on cyber security since the release of the current Cyber Security Strategy that have impacted the sector, across the Federal and State/ Territory levels of government. AustCyber has encouraged and supported the industry to share its views on a number of these[xiv].

Cyber security is a strategic risk for every sector of the economy. It is not just regulation specifically directed at the cyber security sector that industry needs to respond to and manage for/ with their customers. This creates opportunity for the cyber security industry, as much as it is creating friction in managing different requirements of different legislation across sector and layers of government. In some instances, this friction is giving rise to potential unintended vulnerabilities and systemic weakness.

Further, the cyber security industry must also take account of additional international regulatory requirements in being part of the technology capability sets that support national security and intelligence. In some contexts, these requirements need to be considered even if the cyber security company is not directly exporting its products and/ or services.

It is important that all Australian governments and regulators are mindful of the contextual nature of cyber risk as well as the pace at which technology is changing. Many parts of industry agree regulation is necessary and can be beneficial – but the right balance and approaches are needed.

The 2020 Cyber Security Strategy provides Australia with a timely opportunity to provide for a wide ranging assessment of the cyber security implications of Australia's legislative and regulatory frameworks and regimes, across its levels of government; and the implications of Australia's legislative and regulatory frameworks and regimes on the cyber security industry.

There would be benefit in such an assessment also looking at the relative and comparative behavioural impacts of the Notifiable Data Breaches Scheme and *Security of Critical Infrastructure Act 2018 (Cth)* to understand where more could be done to reach affected organisations not yet mature in managing their obligations. There will also likely be case studies of positive behavioural change that can 'show what good looks like' to others across different sectors and contexts.

There is also an opportunity for reform to how all legislation and regulations are developed, reviewed and amended to take better account of both the economic and national security considerations of cyber security – as seen in other countries.

AustCyber also supports in full the recommendations made by Standards Australia to the Department of Home Affairs for the 2020 Cyber Security Strategy consultation. As a further comment, Australia should seek to apply a principle of harmonization between government developed and industry generated practice guidance, noted in our paper on this topic released in 2018[xv]. Uptake of these recommendations would support greater global competitiveness of Australian cyber security companies and encourage closer alignment between policy on cross jurisdictional cyber challenges.

We suggest consideration also be given to the formal feedback loops that could be formed between Government and industry, perhaps through the partnership between Standards Australia and AustCyber, on current and emerging regulatory matters discussed in the Council of Australian Governments and related fora as well as multilateral fora, in particular those between Australia, Canada, New Zealand, the United Kingdom and the United States.

Leadership and coordination: #gameon

Reflections on the Discussion Paper's questions 2-4, 24

The cyber security industry strongly encourages the reappointment of a Minister for Cyber Security. It provided a clear entry point into Government for industry and the research community domestically and internationally, effective coordination of issues and challenges at home and abroad as well as having clear benefits for collaboration across Government, including with the Industry, Communication and Education portfolios. Reinstating a Minister for cyber security would also help clarify the related but different functions of cyber security and cyber safety in the economy and community.

Referencing the 'Regulatory evolution' section above, relevant information shared between parliamentary committees and inquiries regarding cyber security should be published as appropriate. This would help support better coordination within and between Australian parliaments and help ensure the economic and social considerations are better accounted for in national security and vice versa. This would also help improve transparency, provide a useful source of information for policymakers and in the economy for business/ organisational strategy and research – and help to start normalising cyber security practice as an everyday aspect of life.

The following are views provided to AustCyber by a number of its industry stakeholders, including from a number of other sectors of the economy, of which AustCyber supports, on the need for continued leadership from governments, industry and the research community.

- The current Cyber Security Strategy provided stability that previously did not exist. It will be important for domestic contexts but also our positioning globally that the 2020 Cyber Security Strategy reinforces the leadership roles in and out of Government that work in partnership to deliver on the mutually beneficial 'protect' and 'grow' missions for cyber security.

- As a country, we now know just how important cyber is to the resilience of the economy generally. Responsible government bodies still do not appear to have this in mind as they go about their business – leadership and structures need refining to ensure the seeming competition between national security and all else is phased out.

    - The culture of information sharing is still hostile especially on the Government side and under appreciates the willingness of industry (even contracted partners).

    - Stealing of say $30,000 through cyber means consistently does not appear to warrant a response, but that happening in offline crime would have several resources applied and could see an individual/ family fall into bankruptcy or a microbusiness fail.

- There is strong evidence the operational relationship between the Australian Government and the State/ Territory governments has deepened since the release of the current strategy. There would be benefit in more coordinated communication from this collective when breaches and compromises occur, to help normalise the way the broader economy treats cyber security – like emergency management of physical hazards, for example.

- There is a significant opportunity for better coordination of the Joint Cyber Security Centres (JCSCs) and the delivery of activities within them. With an adjustment to the business model and operating principles, the JCSCs could be a significant asset for Government.

AustCyber: our nation’s not so secret weapon

AustCyber is globally unique.

There is no other entity in the global cyber security landscape that is structured, funded or positioned like us. We have become globally recognised as best practice on generating and growing cyber security innovation and industry that has benefit for both economic development and strategic interests.

We hope our time as being the only one of our kind internationally will soon change. Over the last two years, we have provided advice to dozens of countries around the world on how they might establish a like-organisation.

We have briefed the World Economic Forum’s Centre for Cybersecurity on our structure and programs and are a member of its Ecosystem Working Group. We have advised the United Nations Institute for Disarmament Research on the concept of industry development as a form of deterrence in cyberspace. Further, AustCyber has formed partnerships with the MITRE Corporation and the United States National Institute of Standards and Technology on their National Initiative for Cybersecurity Education. As noted above, our work on cyber security workforce development has also seen us become a member of the Global Forum on Cybersecurity Expertise, with our approaches and dashboards being considered for capacity building efforts globally.

Being unique domestically has enabled us to quickly build trust and rapport with cyber security companies, buyers, investors, researchers and community based organisations. It has also supported trusted partnerships with State and Territory governments to build a national network of Cyber Security Innovation Nodes and be a partner of choice on a range of programs and activities across Australian research, innovation and education. These partnerships embody AustCyber’s focus on supporting Australia to capitalise on the multiple benefits of a mature cyber security industry.

Our approach to industry growth and innovation has enabled Australia to not only catch up to many other parts of the world, but also now lead on the models and frameworks supporting sustained growth. Importantly, Australia is also now a credible leader on some cyber capability types and has a strong pipeline of potentially high value startups and early stage companies.

AustCyber has become a critical point of coordination for industry creation and sustainment, forming a key part of the nation’s approach to better managing cyber risk and supporting the economy to become cyber resilient.

As described by several of our ecosystem companies, “The small investment of public money in AustCyber has undeniably delivered in spades, there has been is at least an eight to 10 times return so far. It has been so successful that AustCyber’s funding is now limiting it fully supporting the industry it has grown – the industry has scaled significantly and a good number companies within it are at least five times larger, for the right reasons, but AustCyber’s funding has not grown with it. The timing of AustCyber is right, the model is right; we need AustCyber to be able to continue in its current form but at the right scale to drive home the next phase of sector maturity and grow our competitive advantage.”

The combination of recommendations made in this submission means that looking ahead, the 2020 Cyber Security Strategy would be well positioned on the intersection of the protect and grow missions to work in concert with other efforts underway in governments, industry and the research community. This would enable the country to use the window of current opportunity described above to embed and leverage foundational mechanisms for sustained achievement of outcomes.

What does mission success look like for us?

- Sustained sector growth and maturity supported by AustCyber's 'ideation to export' knowledge infrastructure which includes sophisticated elicitation of the economy's and national security's cyber security problems/ challenges and is supported by a sustained pipeline of skilled professionals

- A high number of globally competitive companies selling domestically to underpin growth and trust in/of other sectors with high uptake of cyber resilient digitalization

- Expanding and exporting cyber capability well above OECD average

- Growth in a globally competitive cyber security workforce and cyber competencies embedded into digital skilling across all sectors of the economy

- AustCyber's sectoral knowledge and expertise is leveraged to shape and influence the policy and regulatory landscape in support of the above.

The corporate aspects

AustCyber – the Australian Cyber Security Growth Network Limited – is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, or in more detail – support the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhance Australia's future economic growth in a digitally enabled global economy as well as to improve the sovereign cyber capabilities available in defence of the nation.

We form a part of:

- the Government's Industry Growth Centres Initiative established through the National Innovation and Science Agenda. AustCyber is one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia

- the current Cyber Security Strategy as a coordination mechanism of cyber security R&D, innovation and industry growth innovation. 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 AustCyber Projects Fund which provides grants to single or consortia projects that deliver national benefit. We also receive funding under contracts with the governments of the Australian Capital Territory, New South Wales, South Australia, Tasmania, Western Australia which we match to deliver in partnership AustCyber's national network of Cyber Security Innovation Nodes – with Queensland and Victoria 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 cyber security 'hot spots' around the world.

Further, with multinational companies that AustCyber engages with, we help to establish productive pathways into Australia's cyber security ecosystem through a range of mechanisms suited to the commercial interests and capability types provided by those companies (often in partnership with Austrade and State/Territory governments).

This has strengthened the breadth and depth of our networks that can be leveraged by Australian cyber security companies as part of their growth strategies and by other organisations in expanding Australia’s impact on the global stage for cyber security and related fields.

[i] Australia’s Cyber Security Sector Competitiveness Plan 2018 Update; Forbes 2019: Top 10 Cybersecurity Companies to Watch in 2019

[ii] Report no longer available online, but quoted at https://www.mailguard.com.au/blog/mid-size-companies-cyber-attack

[iii] Bugcrowd is a global company born in Sydney, New South Wales

[iv] Dtex Systems is a global company born in Adelaide, South Australia

[v] Kasada is an Australian company operating in Australia and the United States

[vi] Nuix is a global company born in Sydney, New South Wales

[vii] Telstra is an Australian company operating globally. AustCyber acknowledges areas of Australian governments are aware of Telstra’s annual security reports

[viii] AustCyber’s 2019 Update to Australia’s Cyber Security Sector Competitiveness Plan, expected to be released in December 2019, will provide a ‘deep dive’ on measuring cyber security in much the same way as the 2018 Update provided a ‘deep dive’ on cyber skills and education

[ix] https://ieeexplore.ieee.org/document/6493323

[x] Under the Industry Growth Centres Initiative, the other five growth sectors are advanced manufacturing, energy resources (including oil and gas), food and agricultural technologies, medical technologies and pharmaceuticals, mining technologies. AustCyber also has partnerships with comparative iniatives in defence industry, space and financial services.

[xi] Based on sentiment and engagement analysis

[xii] https://www.afr.com/technology/bgh-capital-backs-major-new-cyber-security-player-20191010-p52zjv

[xiii] https://www.cio.com.au/article/664947/fifth-aussie-cisos-suffering-from-burnout-report/

[xiv] In being funded by the Government’s Industry Growth Centres Initiative, AustCyber is required to identify areas of regulation that are barriers to the growth of Australia’s cyber security and suggest ways these could be addressed

[xv] Located at https://austcyber.com/news-events/harmonising-cyber-security-guidance