

1 November 2019

Australia's 2020 Cyber Security Strategy Consultation
Department of Home Affairs
3 Lonsdale Street
BRADDON ACT 2612

By upload to consultation website

Dear Sir / Madam

Consultation on development of Australia's 2020 Cyber Security Strategy

The Australian Investment Council welcomes the opportunity to contribute to the consultation process for the Department of Home Affairs' development of Australia's new 2020 Cyber Security Strategy.

The Australian Investment Council is the voice of private capital in Australia. Private capital investment has played a central role in the growth and expansion of thousands of businesses and represents a multi-billion-dollar contribution to the Australian economy. Our members are the standard-bearers of professional investment and include: private equity, venture capital and private credit funds, alongside institutional investors such as superannuation and sovereign wealth funds, as well as leading financial, legal and operational advisers. Our members are comprised of both Australian domestic and offshore-based firms.

Private capital fund managers invest billions of dollars into Australian companies every year. For the first time in history, Australian-based private equity and venture capital funds under management topped \$30B in 2018, testament to the growth in available capital to support investment into businesses across every industry sector of the economy. Fund managers secured an impressive \$6.6B in new investment commitments over the past year, which means the industry has a combined total of around \$11B in equity capital available to be invested in the short-term.

These figures highlight just how attractive the private capital market is to both local and offshore investors. Private capital investment offers an opportunity to provide smart capital to privately back companies in a relatively low-risk environment.

More and more businesses are choosing to raise capital from private investors today, rather than through public markets, because of the benefits of partnering with venture, private equity and private credit firms. Private capital investors can help unlock the growth and expansion opportunities of businesses through active asset management, in a way that public markets simply cannot.

All sectors of the economy have a role to play in informing and engaging with the government on important issues that will help to improve the productivity and competitiveness of businesses domestically and internationally. This includes our private capital investment industry, which invests in a wide range of Australian businesses, be they early stage tech startups, or long-established agricultural, manufacturing or services-based businesses. In particular, our private equity, private credit and venture capital fund manager members seek to invest in high-growth companies that use that invested capital to expand their workforce, increase sales growth and invest in highly innovative and market-leading research and development.

Policy recommendations aimed at enabling these scale-up businesses to succeed and become internationally competitive should be complemented by innovation-focused initiatives that can have a significant impact on Australia's broader economic transformation. These include creating the next wave of



global, Australian-based businesses to drive our transition towards more highly skilled, well-paid jobs and to an economy that is well protected from cyber threats.

In the context of the cyber security and data privacy sector, we expect to see continued growth in the extent of private capital investment to keep Australia at the forefront of international developments and to capitalise on our relative strength in capability in this area. The development of Australia's 2020 cyber security strategy should recognise the opportunity to drive that growth through a strategic roadmap for the next decade. The new strategy should also promote and prioritise improvements in our education system which will support the ongoing development of our future pipeline of skilled talent in the cyber and data privacy area, which is essential for the protection Australia's infrastructure and security over the long-term.

Other national strategies developed in comparable markets, such as the United Kingdom, have taken the opportunity to set out how they will acquire and strengthen the tools and capabilities that their market needs to protect itself from the cyber threat. We encourage the Australian government to adopt a similar approach to consideration of the key features that should be incorporated into the development of our new national strategy for 2020 and beyond.

Australia is a predominantly services-based economy underpinned by technology

The Australian economy is today a predominantly services-based market, which increasingly, is becoming more and more dependent on our ability to access technology and data networks and to develop new innovations that are protected from cyber risks.

There is no question that cyber 'attacks' are becoming more prevalent across all spheres of government, business and society. The level of sophistication continues to increase, and the impact of such attacks can be catastrophic, especially in the context of highly sensitive sectors such as defence, as well as healthcare, infrastructure and personal security. The expansion of internet-capability beyond computers and mobile phones into other cyber-physical or 'smart' systems is extending the threat of remote exploitation to a host of new technologies which underpin the everyday lives of Australians such as transport control systems, power grids and industrial plants.

Managing Australia's exposure to cyber risks relies on our capacity to access the right skills and talent, and our ability to support greater investment into research, leading to the development of innovative solutions.

Australia's venture capital investment sector is a key driver of innovation investment across the domestic economy. Investing today into the businesses of tomorrow is a core ingredient in creating a more knowledge-based and high-value-add economy in the 21st century.

Education and training are also essential. According to analysis completed by AustCyber, there is a significant shortage of job-ready cyber security workers in the local market, with the need for an additional 17,600 cyber security workers anticipated by 2026 to fulfil Australia's growing cyber security and data privacy requirements. Central to the required growth in labour is the need to ensure we develop a larger pipeline of successful cyber and data security firms over the next decade. Growing the number and scale of businesses in this sector will go a long way to creating new employment opportunities for the next generation of Australians that we need to meet the demand for talent in this area. The downstream pay-offs for the Australian economy, and for Australian consumers, will be substantial.

The role of private capital investment in growing Australia's cyber business capability

There is a significant and important role that government can play alongside industry in seeking to support Australian consumers in managing cyber security risks across many dimensions of everyday life.

An important driver, from our perspective, is to continue to strengthen our domestic cyber security industry capability through home-grown enterprise and talent. Doing so will have a direct impact on continuing to lift



consumer awareness and engagement in this area through greater public dialogue of cyber security and risk across all corners of society.

The decision by the government to establish AustCyber in 2017 was a profoundly important one.

The role that AustCyber has been created to play, in aligning disparate cyber security initiatives and investments across the business sector, the research community, academia, and governments in Australia, will help to accelerate the growth of our domestic capability into the future. Government should continue to support its long-term investment into AustCyber, allowing the role that it currently plays to build and expand as our sector capability in the cyber security area grows over time. The relatively modest investment of public funding into AustCyber will deliver exponential returns to the Australian economy, and society, on an enduring basis into the future.

However, more can – and should – be done to support and complement AustCyber’s efforts.

Of particular importance to us is 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. Boosting the level of investment will serve the dual purpose of:

- creating greater access to relevant products and services for consumers to manage key areas of risk confronted on a daily basis, 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.

Encouraging greater private capital investment

AustCyber’s mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia’s future economic growth.

Development of the nation’s new 2020 cyber security strategy should recognise and complement AustCyber’s role in addressing key aspects of how Australia will respond to the challenges confronted in the cyber and data privacy area right now, and over years to come. The new strategy should incorporate a focus on developing policies and initiatives that directly or indirectly encourage growth in the flow of capital investment into the sector over time.

Analysis of global data across our industry reveals that the ‘internet of things’ and ‘digital technology’ sectors have attracted more than US\$33B in new venture capital investment across developed markets in the nine months to 30 September 2019. Reliable conservative estimates of the extent of cyber security investment within that number suggest that perhaps 15-20% of the total invested capital has flowed into cyber security. Key offshore markets such as the United States and Israel tend to dominate the global weight of capital moving into the cyber security and data privacy sector. Australia has recognised the opportunity to capitalise on the underlying strong footprint we have in the cyber and data privacy sector, but as AustCyber has identified in their current Sector Competitiveness Plan (SCP):

“Australia offers an ideal growth environment for cyber businesses, thanks to strengths in core research areas like quantum computation, wireless technology, trustworthy systems and niche high-value hardware. Further drawcards for investment include Australia’s large services economy, quality education system, sound governance settings, economic stability, low sovereign risk and high living standards. The proximity to the fast-growing and increasingly digitised Indo-Pacific region adds to Australia’s natural advantages.

...

Several hurdles are making it difficult for Australia to fully exploit existing advantages and develop a sizeable world-class cyber security sector. To harness the enormous opportunity in cyber, Australia must



address the skills shortage, focus efforts in research and development, improve the environment for incubating startups, and work to enhance access to global markets.”

[AustCyber 2018 Sector Competitiveness Plan]

In our view, boosting the level of private capital investment into this sector requires a targeted and strategic focus that is supported through co-ordinated policy, regulatory and market-based solutions.

AustCyber’s SCP identifies the existing barriers that constrain Australia’s capacity to grow more businesses in the cyber security sector. The barriers identified are:

- a shortage of job-ready workers
- a lack of focus in research and commercialisation, and
- barriers to growth and export for smaller local cyber security providers.

Cyber security and data privacy currently represents a modest, but growing, component of the overall mix of venture capital invested into the technology and digital sector in Australia. Growing the proportion of capital moving into the cyber and privacy area will be driven by three key factors in our opinion:

1. Encouraging greater patient capital investment through fund managers and institutional investors
2. Attracting more offshore investment into Australia’s cyber security sector
3. Improving links, knowledge and skills shared between researchers, entrepreneurs and investors.

Over recent months the Australian Investment Council has taken steps to establish a closer collaboration with AustCyber, to support areas of common interest that can be developed together to enhance and expand the role of Australia’s cyber security sector within the economy and society.

So far, we have identified two key impediments to growing the quantum of private capital investment into the cyber security and data privacy sector in Australia, they are:

- 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 the early-stage cyber security business sector and the established private capital investment sector both here in Australia, and abroad.

In seeking to tackle the impediments outlined above, we believe it is instructive to look at the work completed by the United Kingdom in recent years as part of the development of their 2016-21 national cyber security strategy. The UK has taken the opportunity to set out how they will acquire and strengthen the tools and capabilities that their market needs to protect itself from the cyber threat. They are doing this through a range of initiatives aimed at creating an ‘ecosystem’ that allows businesses in the sector to prosper, collaborate with research institutions and institutional investors, and bring the weight of ‘government-as-a-customer’ to help drive commercial activity.

In the UK strategy, developing this deeper and more strategically aligned ecosystem is promoted and prioritised as an important ingredient in their approach towards effectively managing the country’s exposure to cyber risk.

‘Government-as-a-customer’ to drive growth in the cyber sector

Governments around the world are typically exposed to some of the most significant cyber security and data privacy threats from domestic and offshore instigators. There is a compelling argument, therefore, that government procurement can, and should, play a prominent role in Australia’s forward cyber security strategy.

It is generally agreed across our market that government contracts are both highly sought-after, and highly competitive, almost without exception. Because of that, it is important that there continues to exist a robust framework around which the awarding of such contracts is regulated, monitored and managed. In parallel



with that, however, we must ensure that such controls do not present significant barriers to new entrants who wish to participate in the provision of products and services to government.

Additionally, in the context of cyber security, it is important that further consideration be given to balancing the risks associated with the potential for funding to be attracted into such businesses from offshore regimes that do not exhibit the appropriate bona fides that Australia expects.

The new strategy should consider the most appropriate mechanisms through which such a balance can be struck. It may be appropriate, for example, for a framework to be established to set out the specific criteria that should be applied to cyber security businesses in order to protect Australia's interests to the greatest extent possible. Ultimately, the core proposition that must be addressed in this context is to have clarity and transparency around the underlying source of funding and financing. This core proposition should feature in any analysis, regardless of whether or not the regime from which the investment is sourced is considered 'similar' or 'comparable' with Australia.

Maintaining stability of Australia's foreign investment policy regime

Australia's A\$30B private capital investment industry relies extensively on the importation of capital from offshore.

Notwithstanding our large pool of accumulated savings within the domestic superannuation sector, private capital investment is a global asset class that, quite appropriately, attracts investment funding from a mixture of domestic and offshore sources.

Foreign investment into our sector is already monitored and reviewed by the Foreign Investment Review Board. The scrutiny applied by the Board in reviewing the underlying source of investment funds from offshore is extensive and detailed. A number of years ago, changes were made to Australia's foreign investment policy regime that significantly expanded the reach of the Foreign Investment Review Board's scrutiny, especially in circumstances where the underlying source of funds was deemed to be a 'foreign government investor' under the *Foreign Acquisitions and Takeovers Act 1975*.

Ensuring that the policy framework around foreign investment remains both stable and robust is vitally important, in our view. It is one of the mechanisms through which government can maintain Australia's reputation as an attractive and safe destination for investment capital to flow. At all times, the foreign investment policy regime should carefully weigh the need to continue to attract offshore investment into Australia, against the need to protect Australia's national interests – which is could be argued, is especially important in the context of the cyber security and data privacy sector.

Importing skills to fill gaps in capability

Australia is a net importer of not only capital but also, in many cases, skilled talent.

Skilled migration has been a key element of Australia's migration system for decades, playing an important role in generating economic growth across every sector of the domestic economy. While Australia has had a long and successful history of facilitative policies to attract business entrepreneurs, the rising global mobility of workers and heightened competition for talent means that it is important for Australia to continue to improve on past policy settings to ensure we can compete for 'new economy' skilled talent. Doing so in an effective way will enable our economy to continue its transition towards a greater knowledge-based high value-adding market that supports our future productivity, competitiveness and economic growth.

Ongoing improvements to our long-term education outcomes (discussed below), particularly in the STEM disciplines, will help build the next generation of local talent. However, in the short-term, targeted immigration policies will play a vitally important role in facilitating the importation of much-needed specialist skills that do not currently exist, or do not exist to the depth required, in the local labour market.



The global search for talent is compounded by ever-more-rapid changes brought about by technology and innovation. Australia has already identified the need to remain competitive in the race towards attracting the best and brightest talent.

The 2018 changes to replace the previous 457 visa program for skilled labour with the new Global Talent Sponsored program is still in its relatively early phases of maturity. Over time, we expect to continue to see the downstream impact of the new regime, as compared to the historical experience under the 457 visa program. Initial feedback about the new program was mixed – some analysis identified the number of visas granted for developers and programmers dropped 31%, along with a 50% drop for analyst programmers and a 10% drop for software engineers, in the period from July to December 2017 compared to the equivalent numbers in the year prior. However, more recent announcements about the pathway to permanent residency for certain eligible workers under this program has improved the perceived value and attractiveness of the program to an extent.

The Australian Investment Council believes that ongoing monitoring of the effectiveness of the new visa regime should be an important priority to ensure that the capacity for the domestic market to attract skilled talent to support the ongoing growth and expansion of our domestic cyber security and data privacy sector remains competitive.


Developing long-term pipeline of human capital

In a longer-term context – complementing the role of skills-gap policies such as immigration and visa programs discussed above – it is important that Australia’s cyber security strategy continues to support an emphasis on developing human capital through education and knowledge-building initiatives.

Education pathways must place technology at the heart of almost all dimensions of primary and secondary school programs, and government has a role to play at both a federal and state level to support and ensure that this transition is taking place across all communities in a co-ordinated and consistent fashion.

There is no question that today’s children will be confronted with a more digitally-enabled future, and to achieve the ideals of ‘greater consumer awareness’ that the new strategy seeks to address, improving early and later-stage education will go a considerable way towards improving attentiveness and knowledge of cyber security risks over the long-term.

Further information

We look forward to participating in any future discussion about the themes set out in this submission as part of the government’s development of Australia’s 2020 Cyber Security Strategy. If you have any questions about specific points made in our submission, please do not hesitate to contact me on 

Yours sincerely,



Yasser El-Ansary
Chief Executive