Greg Miller
First Assistant Secretary
Cyber Security Policy
Department of Home Affairs
(By webform)

November 8, 2019

Dear Mr. Miller,

Thank you for the extended opportunity to contribute to the discussion paper that will inform the development of Australia's 2020 Cyber Security Strategy.

By way of background, the Digital Industry Group Inc. (DIGI) is a non-profit industry association that advocates for the interests of the digital industry in Australia, with Google, Facebook, Twitter and Verizon Media as its founding members. DIGI also has an associate membership program for smaller digital companies, such as Redbubble, eBay and GoFundMe.

DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected. DIGI's mission is to advocate for policies that enable a growing Australian technology sector that supports businesses and Internet users, in partnership with industry, governments and the community.

We recognise the importance of the issues raised in the discussion paper. "*Australia's cyber security strategy: A call for views".* In response to several of the discussion questions posed, this submission offers several high-level considerations for the Government in informing its areas for further analysis and investment.

DIGI looks forward to further engaging with the Department of Home Affairs' consultation process in relation to the Cyber Security Strategy. Should you have any questions about the representations made in this submission, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

1. What is your view of the cyber threat environment? What threats should Government be focusing on?

In brief, there are a broad range and scale of cyber security threats that necessitate varied Government attention. These range from micro threats that typically target individuals -- such as identity theft or phishing scams to macro threats -- to macro threats, such as hacking and attacks of public and private institutions that have large volumes of data. Such micro threats require a combination of consumer awareness and encouraging industry best practice, through initiatives by Government and industry and collaborations between them. Certain macro threats, such as those that are state-sponsored will require Government focus through a range of Government-led mitigation and response efforts, such as diplomacy foreign affairs.

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Cyber security is an economy-wide issue in a digitally-enabled economy -- it is both relevant to technology companies *and* to companies across all sectors that avail of technology. It is also of crucial importance to all government departments in light of the increasingly digital nature of service delivery. Additionally, mitigating cyber risks is also reliant on informed consumer behaviour at an individual level.

Therefore, there is a strong need to promote cyber security as a shared responsibility across Government, industry and individuals, and clearly defining the role that each must play. A collaborative approach between governments, companies and individuals will be the most effective way to improve cyber security at a macro and macro level. Such an approach would mirror the recommendations of the 2016 Cyber Security Strategy.

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

It is not clear today where the responsibilities for Australians' cyber security lie across Government, as many departments consider elements of it to fall under their remit. For example, it is understood that today responsibilities related to cyber security fall across the Australian Cyber Security Centre in the Australian Signals Directorate, the Attorney General's Department, the Office of the Australian Information Commissioner (OAIC), the Australian Competition and Consumer Commission (ACCC), the eSafety Commissioner, the Department of Communications and the Department of Home Affairs. It therefore is not apparently clear to industry nor individuals which government department would be the lead or appropriate port of call for enquiries relating to cyber security.

In order to assist in creating this clarity and to elevate the importance of cyber security within Government, we would welcome the reintroduction of a Cyber Security Minister. Such a Minister can develop expertise on these issues, act as an advocate within Government for cyber security, and assist in the coordination of efforts across different departments.

In addition, a Minister or a lead agency may also be able to assist in weighing the cyber security considerations in legislation designed to achieve other aims. For example, there is broad consensus among industry and digital rights civil society organisations that the Assistance and Access legislation

poses threats to cyber security as strong encryption serves Australia's national interests by protecting governments, communities, and the economy from criminal, terrorist, and state-sponsored attacks[1].

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

In the most serious attacks, the Government's role is important in both guiding the correct response and public communications. The Government can act as both a trusted adviser to affected organisations and individuals, as well as a spokesperson for attributing attacks.

6. What customer protections should apply to the security of cyber goods and services?

In an increasingly digitised economy, where almost all institutions across Government and the private sector use digital technologies with varying levels of customer data, it makes sense for customer protections in relation to security of digital products and services to be embedded into existing standards that are relevant to particular practices or sectors. This might include laws and codes already implemented by OAIC, the Australian Communications & Media Authority (ACMA), the Office of the eSafety Commissioner or the State Offices of Fair Trading. We understand that the Internet of Things Alliance has developed a security standard for IoT devices that should be more widely considered[2].

7. What role can Government and industry play in supporting the cyber security of consumers?

Both Government and industry have an important role to play in the prevention of consumer risks, through awareness raising and information provision, as well as the mitigation of cyber threats within institutions, as well as the appropriate response after the fact. This is an area where strong collaboration and coordination will improve the effectiveness of such efforts. Government can also act as a role model in the adoption of strong security measures across its digital portfolio and activities.

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

One idea is for Government and industry to promote and adopt existing standards developed by the International Standards Organisation[3], as well efforts to increase consumer awareness of cyber risk mitigation and response.

---

[1] AccessNow, "The role of encryption in Australia", accessed at https://www.accessnow.org/cms/assets/uploads/2018/01/Crypto-Australia-Memo.pdf
[2] IoT Alliance Australia, "Security Guideline", accessed at https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf
[3] International Organization for Standardization, "ISO/IEC 27001 information security management", accessed at https://www.iso.org/isoiec-27001-information-security.html

10. Is the regulatory environment for cyber security appropriate? Why or why not?

There are existing consumer protection and privacy laws that already apply to cyber security. For example, under the Australian Privacy Principles (APP), APP11 relates to the security of personal information. This requires an APP entity to "take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure."[4] In addition, the OAIC has published a "Guide to securing personal information" that it uses to investigate whether an entity has complied with its personal information security obligations[5].

In addition, the Attorney-General's Department has a Protective Security Policy Framework[6] that articulates government protective security policy, including information security. The Australian Signals Directorate has also developed Australian Government Information Security Manual, which outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats[7]. These existing structures should be reviewed and potentially updated in advance of any new regulatory environment being proposed.

Furthermore, as noted, in an increasingly digitised economy, where almost all institutions across government and the private sector use digital technologies with varying levels of customer data, it makes sense for customer protections in relation to security of digital products and services to be embedded into other standards that are relevant to particular practices or sectors.

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

As well as the existing frameworks identified in the response to question 10, one additional consideration might be to examine the Internet of Things Alliance Australia Security Guidelines and how they might be applied more widely, and socialised through efforts between Government and industry[8].

---

[4] Office of the Australian Information Commissioner, "Chapter 11: APP 11 — Security of personal information", accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/#ftn1

[5] Office of the Australian Information Commissioner, "Guide to securing personal information", accessed at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/

[6] Attorney General's Department, "The Protective Security Policy Framework", accessed at https://www.protectivesecurity.gov.au/

[7] Australian Signals Directorate, "Australian Government Information Security Manual", accessed at https://www.cyber.gov.au/ism and https://www.cyber.gov.au/sites/default/files/2019-10/Australian%20Government%20Information%20Security%20Manual%20%28October%202019%29.pdf

[8] IoT Alliance Australia, "Security Guideline", accessed at https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

DIGI recently commissioned research, conducted by the economics firm AlphaBeta, into the state of Australia's technology sector in comparison to other OECD countries. Among many other findings, it included analysis of factors that impact the attraction a talented technology workforce in Australia.

The report finds:

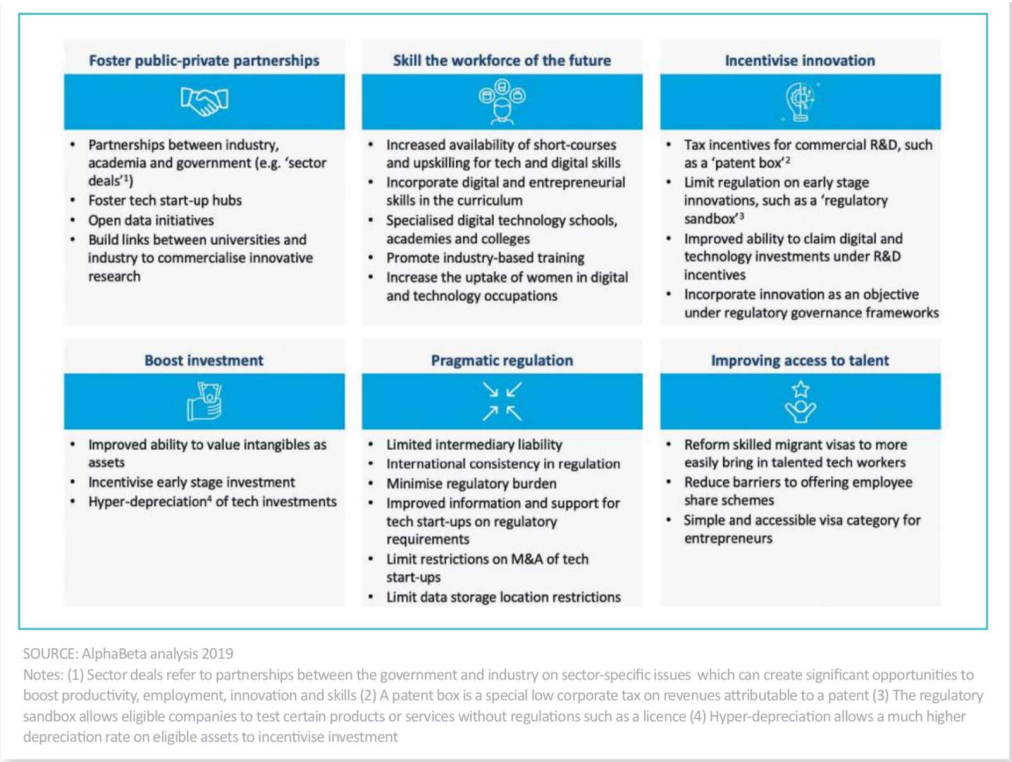
> *The tech sector requires occupational skill sets that may not have existed even five years ago in areas such as data analytics, product development and management, artificial intelligence, machine learning, cybersecurity and robotic process automation. With a relatively limited domestic technology workforce and restrictions on skilled migration, difficulties in finding talented technology workers is leading to many firms restricting their operations in Australia*[9]*.*

Drawing on research from Deloitte Access Economics[10], the report also concludes that Australia's technology workforce in a number of areas including cyber security had to grow at least twice as quickly in order for Australia to be globally competitive in this area. It identifies relevant barriers to talent acquisition in these areas, noting "bringing in experienced overseas talent is often necessary to help mentor and grow local talent. Australia's visa system makes this difficult. For example, the Temporary Skills Shortage visa defines occupations using ANZSCO codes, which do not include many new tech sector occupations." In this context, initiatives such as the Australian Government's Australian 12-month pilot for a Global Talent Scheme are welcome, and further analysis should be undertaken to examine the impact of such initiatives, as well as relevant global initiatives such as those outlined in *Australia's Digital Opportunity,* in building a market of high quality cyber security professionals in Australia.

More broadly, the report identifies six policy conditions, as outlined in Figure 1 (overleaf), that have an impact on various aspects of the sector, all of which should be examined in attempts to better understand contributing factors to the talent pool of cyber security professionals in Australia.

[9] AlphaBeta (September 2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf
[10] Deloitte Access Economics (2018), "ACS Australia's Digital Pulse", accessed at https://www.acs.org.au/insightsandpublications/reports-publications/digital-pulse-2019.html

Figure 1



SOURCE: AlphaBeta analysis 2019

Notes: (1) Sector deals refer to partnerships between the government and industry on sector-specific issues which can create significant opportunities to boost productivity, employment, innovation and skills (2) A patent box is a special low corporate tax on revenues attributable to a patent (3) The regulatory sandbox allows eligible companies to test certain products or services without regulations such as a licence (4) Hyper-depreciation allows a much higher depreciation rate on eligible assets to incentivise investment

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

As noted, there are a broad range of cyber security threats that range from macro threats -- such as hacking and attacks of public and private institutions that have large volumes of data -- to micro threats that typically target individuals, such as identity theft or phishing scams to macro threats. On the latter, this is an area where industry, Government should closely collaborate to raise public awareness and education on cyber risk mitigation, management and response.