IBM Centre
601 Pacific Highway
St Leonards NSW 2065

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit
Barton ACT 2600
Via online Submission

31 October 2019

Australia's 2020 Cyber Security Strategy

Thank you for the opportunity to comment on Australia's proposed 2020 Cyber Security Strategy. We commend the Australian Government for seeking industry and wider input into this important area.

IBM supports the statements made in the submission of the Business Software Alliance, of which we are a member. In particular we recommend that the Australian Government incorporate the six guiding principles noted in that submission in updating the 2020 Cyber Security Strategy, namely that in developing the Strategy it should ensure the following;

1. Policies Should Be Aligned with Internationally Recognized Technical Standards. Internationally recognized technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cyber security, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. Alignment with internationally recognized technical standards and guidance, as such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report 27103, can ensure that Australia benefits from proven approaches to cyber defence and is even better-positioned to cooperate inter-operably with the international community in confronting transnational threats, especially with respect to the protection of systems for delivering essential services .

2. Policies Should Be Risk-Based, Outcome-Focused, and Technology-Neutral. Malicious cyber security activity carries different risks for different systems. There are generally multiple approaches to defending against the same type of cyber attack, and multiple approaches to improving system security and resiliency. The 2020 Strategy should prioritize approaches and policies that address different levels of risk and enable owners and operators of networks and systems to defend their infrastructure with the technologies and approaches that best meet the level of security required.

3. Policies Should Rely on Market-Driven Mechanisms Where Possible. Information technology is constantly evolving, and cyber security threats evolve with it. Neither technologies nor threats are bound by national borders, meaning that overreliance on government structures or regulatory enforcement is unlikely to be sufficient to manage threats. Policies that incentivise and leverage market forces to drive cyber security are likely to be most successful in keeping pace with the changing security environment and in achieving the broadest effect.

4. Policies Should Be Oriented to Protect Privacy. No approach to cyber security should compromise the integrity of the data it seeks to defend against malicious cyber activity; cyber security policies should be carefully attuned to privacy considerations. Key considerations include ensuring civilian leadership, encouraging strong data protections, protecting personal information in information-sharing mechanisms, and avoiding policies that

undermine the use of privacy-enhancing technologies. Australia has already taken a commendable principles-based, outcomes-focused approach to privacy and personal information protection, primarily through the Australian Privacy Principles. The 2020 Strategy should continue to embrace the enabling effect that this principles-based approach has had on innovation and development of the digital economy in Australia.

5. Policies Should Be Flexible and Adaptable to Encourage Innovation. Information technology and the millions of jobs technology supports depend on the ability to innovate new solutions. Cyber security requires constant innovation to keep pace with changing threats. Policies must be flexible and adaptable to enable businesses to develop new approaches to new challenges and to deliver innovative products to the customers that depend on them, and we commend the Australian government for already recognizing the need for flexible laws in this regard.

6. Policies Should Be Rooted in Public-Private Collaboration. Cyber security is a shared responsibility across government and private stakeholders. Although governments often hold critical cyber security tools and information, the private sector is responsible for significant elements of the critical infrastructure and the technology platforms that are targeted by malicious cyber activity, as well as many of the cyber security tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can governments truly combat cyber security threats while sustaining the vitality of the digital economy. In this respect, we are pleased to note that the Discussion Paper already calls out the need for the 2020 Strategy to be developed and supported through partnership and collaboration with the industry.

In relation to public and private collaboration, IBM believes that the focus in the 2016 Strategy, whilst a very good start to this complex area, was focussed on engaging and developing the local Australian cyber security industry. Whilst IBM understands and appreciates the importance of this policy objective, we would also like to stress that preparing and responding to Cyber security threats is a global challenge. Cyber attacks often involve multiple operatives from across a global network targeting multiple enterprises around the world at the same time. Many of these enterprises are managed by the private sector and large multinational corporations in particular. Therefore global government and industry cooperation is critical in order to successfully minimise and respond to cyber-crime.

Whilst it is well accepted that a strong local cyber security software industry is important, we recommend that the Government put in place a more inclusive engagement with global cyber security vendors who have sophisticated onshore research facilities, highly qualified and expert staff who are responding to cyber incidents with Australian companies on a regular basis. Some of these global companies, such as IBM, have made significant investments in Australia and have much to contribute in terms of expertise, research and skill development as out lined below.

The IBM Australian Development Laboratory

IBM is a global leader in cyber security which has invested heavily in research, technology and services over many years. In particular it has made significant investments to develop this expertise in Australia, including establishing the Australian Development Lab on the Gold Coast in Queensland. The location is also part of story of an Australian cybersecurity start-up that has successfully integrated into a global corporation and remained vital and relevant for 20 years.

The Australian Development Laboratory is now a leading Security development centre within the IBM global enterprise and delivers key technology and expertise that is made available to public and private clients in Australia and around the world. With a staff of around 90 security software engineers, master inventors, the IBM Australian Development Laboratory has combined an agile start up culture, Australian creativity, deep security expertise and collaboration with the IBM global security research and software development community.

Being a part of a global cyber security network enables the IBM Australian Development Laboratory to:

- invest and make available substantial cyber research;
- access vast amounts of global cyber security capability in real time;
- develop open standards that facilitate collaboration and capability adoption;
- invest in global product engineering within Australia;
- employ significant numbers of Australian cyber security professionals;
- partner with local Australian cyber security firms;
- obtain Australia security patents and commercialise assets ; and
- contribute substantially to developing cyber skills and talent through its relationships with Griffith University, the University of Queensland ad Southern Cross University.

In addition, the IBM Asia Pacific headquarters for IBM's X-Force services is in Melbourne, Victoria. This capability delivers world class services in the identification of vulnerabilities in core systems of clients, and also responds to some of the most severe breaches occurring in Australia and globally. The IBM team currently engage directly with the ACSC during these incidents, but we strongly believe that there are significant mutual benefits of expanding this limited engagement to a more structured and ongoing dialogue.

IBM therefore urges the Government to include in its 2020 Cyber Security Strategy a mechanism that enables global companies with significant Australian development and research investments to more fully participate and collaborate in the Australian cyber security eco-system, share data, research, expertise and skill development strategy. We believe that the IBM Australian Development Laboratory and the X-Force Services team in Victorua have much to offer in this area and would welcome the opportunity to do so.

Cyber Security Policy Environment

Whilst IBM does not have particular issues to raise in relation to most of the specific questions asked in the discussion paper, we do wish to comment on Question 10, which asks "is the regulatory environment for cyber security appropriate?"

In general, IBM believes the Australian government has created a regulatory environment that promotes strong cyber security without constraining innovation or digital commerce. However, this has been undermined by the government's adoption of *the Telecommunications (Assistance and Access) Act 2018* which has created concerns about Australia's ability and commitment to embrace the most effective cyber security policies and technologies.

Strong encryption represents a critically important cybersecurity technology. It underpins data security, identity management, and protection of devices against unauthorized access. It also plays a crucial role in defending critical infrastructure systems. Yet, notwithstanding limitations on mandating the weakening of encryption within the legislation, the Australian government has introduced 'Technical Assistance Notices' within the Assistance and Access Act in a way that undermines investment in cyber security in Australia. Security experts around the world have recognized that empowering law enforcement agencies to build technology to counter encryption will result in a weakening of the encryption technology in use.

As the Australian government considers its 2020 Strategy, it must pursue policies that address both the threats of today and the threats of tomorrow. Promoting strong and ubiquitous encryption is essential both now and into the future. As Australia embraces 5G technology, for example, encryption – and end-to-end encryption, particularly – will take on even greater importance as a way to protect massive volumes of data traversing increasingly decentralized, potentially untrusted network infrastructure. Likewise, encryption has also been identified as key to securing the Internet of Things.

To position the Australian government to embrace technologies that will best protect Australia from malicious cyber attacks, IBM urges the government to review the provisions of the *Telecommunications (Assistance and Access) Act 2018* to clarify the important and

potentially damaging consequences for cyber security investment in Australia, particularly those that arise from the current operation of 'Technical Assistance Notices'.

If you require any clarification or further information in respect to any matter related to this submission, please contact Mr Christopher Hockings, IBM CTO Security Australia & New Zealand at [redacted] or myself.

Yours sincerely

[redacted]

Kaaren Koomen AM
Director, Government & Regulatory Affairs
IBM Australia & New Zealand