1 November 2019

Hon Peter Dutton MP
Minister for Home Affairs
House of Representatives
PO Box
Parliament House
Canberra ACT 2600

Dear Minister

UNSW submission to the Department of Home Affairs' *Australia's 2020 Cyber Security Strategy* discussion paper

The University of New South Wales (UNSW) welcomes the opportunity to provide input to the development of Australia's 2020 Cyber Security Strategy.

UNSW is one of Australia's leading research and teaching universities and is currently ranked 43rd in the 2020 QS World University Rankings. Through its *2025 Strategy*, UNSW is committed to research that addresses some of the most significant challenges facing Australia and the world, as well as educating students to become highly employable skilled professionals.

Of particular relevance to this submission, UNSW is recognised as a leader in the field of cyber security. UNSW is currently ranked first in Australia for Telecommunications Engineering (2019 Academic Ranking of World Universities Subject Ranking) and first in Australia and 38th globally for Engineering and Technology (QS World University Subject Ranking). We are a founding partner of the Cyber Security Cooperative Research Centre, and this year hosted the inaugural Australian Cybersecurity Education Summit which brought together leading cyber educators, industry and government professionals.

UNSW looks forward to working together with Government to improving Australia's cyber security capability, and to ensuring that *Australia's 2020 Cyber Security Strategy* best delivers its intended outcomes for the nation.

Universities and cyber security

UNSW is well-placed to provide input to *Australia's 2020 Cyber Security Strategy*. As educators of cyber security professionals, universities are important stakeholders in addressing the cyber skills shortage in Australia. Our world-leading cyber academics and experts contribute regularly to policy discussions on current best practice. Universities work closely with industry to develop new knowledge in cyber and to innovate new technologies, practices and systems. And, as the discussion paper acknowledges, universities themselves are institutions of national importance that are often the target of malicious cyber activity.

UNSW's own cyber security continues to be one of the University's highest priorities, and we are working closely with the Government, including Minister Tehan's recently announced University Foreign Interference Taskforce, aimed at building on existing safeguards against foreign interference to maintain and improve cyber resilience through a collaborative process. While there has recently been significant focus on issues relating to foreign interference, it is important to note that that this is but one dimension of cyber security in a university context.

2016 Cyber Security Strategy

Revising the 2016 Cyber Security Strategy is timely and necessary given the rapid pace of technological change and evolving threat environment. The discussion paper correctly asserts that the Government must work in partnership with the Australian community to develop and deliver *Australia's 2020 Cyber Security Strategy* for it be successful. UNSW is pleased that a diverse range of issues relating to Australia's cyber environment are 'on the table' for discussion, including the role of government in deterring, detecting and responding to cyber threats as well as the need for industry to bear greater responsibility of cyber risk.

UNSW suggests that the next iteration of the national Cyber Security Strategy should be more selective in focus than it was in 2016 and more fully resourced. Noting that phishing and business compromise are some of the most significant cyber security risks in Australia, UNSW suggests that accordingly, the primary focus of *Australia's 2020 Cyber Security Strategy* should be to promote a better understanding of risk management processes for Australian businesses.

Role of the government

While considerable progress has been made since 2016 towards establishing a clear role for government, such as creating the Australian Cyber Security Centre (ACSC) and establishing the Australian Signals Directorate (ASD) as a statutory agency, there are still a range of policy and legal settings that the Government needs to address. Furthermore, the ACSC needs to be properly resourced, while gaining an understanding of how best to make it 'fit for purpose'.

A range of Australia's critical infrastructure, such as hospitals, water and electricity utilities, transport networks and telcos are increasingly digitally enabled. The strategy needs to articulate this and address the risks inherent in public infrastructure. The National Broadband Network (NBN) in particular offers the possibility to form part of the solution, either through its initial development, or retro-fitted at a later stage.

It is clear that the Government is seeking to gauge the level of support for expansion of its powers to deter, detect and respond to serious cyber threats within Australia. Cyber events in recent years have exposed weaknesses in some of Australia's institutions and clearly make a strong case for greater Government-led prevention and intervention.

However, the detail of any legislative changes to the Government's cyber capabilities domestically must be carefully scrutinised and evaluated against the impact on security, privacy and other rights and would reasonably be expected to be used in limited circumstances and include appropriate checks and balances beyond Ministerial discretion. There is the risk that regulation could also become problematic and create an unnecessary 'red tape' burden if it is not designed properly.

Although legislatively there is a limit to what activities the ASD can currently undertake domestically, it is understood that operationally ASD does currently provide technical advice to other agencies for domestic cyber activities. The Government must make a clear case for the need to expand ASD's role.

The debate around encryption laws highlights the tension between the Government seeking expanded law enforcement powers and the privacy rights of citizens and speaks to the issue of trust as is mentioned in the discussion paper. The Government must consider that its position on encryption may impact the public's perception of further changes to the Government's cyber security powers.

While legislating an expanded role for Government to respond to serious cyber threats may improve cyber security within Australia to some extent, the fact remains that the Government alone cannot be responsible for maintaining and building cyber security in Australia. In fact, it would be a step backwards if increased capabilities for Government were to contribute further to a sense of complacency in organisations.

The legal framework is a critical element of the Government's role in cyber security. The current legal framework is at times patchy and poorly applied. The payment card industry compliance scheme is a good framework to base the regulation on. Furthermore, breach reporting is an important element of the law, as it provides an incentive for each party to properly protect data.

Shared responsibilities between industry and government

UNSW agrees that cyber security is a shared responsibility between government, industry and the Australian community. The 2020 Cyber Security Strategy must contain clear responsibilities that lie with the party best able to address each issue and should not be used for Government to transfer risk to universities and the private sector unduly. The benefits and risks are collectively shared between Government, industry and universities.

Responsibility for some cyber security requirements are naturally going to be shared between government and industry, with the optimal solutions only achieved through close collaboration. Some shared responsibilities include implementing authenticated email, such as Domain Message Authentication, Reporting and Conformance (DMARC) and Sender Policy Framework (SPF) to eliminate phishing scams.

At a policy level, it should be noted that there is a reasonable 'sovereignty' argument to promote the manufacture of hardware and software in Australia. The inclusion of this kind of policy would aim to protect the nation from cyber attacks by ensuring the supply chain is subject to appropriate regulations and scrutiny under Australian law. A similar argument has previously been used with regard to the automotive industry and indeed the manufacture of certain defence hardware in Australia.

The role of industry

As the discussion paper explains, the role of industry needs to be addressed to shift risk away from consumers, who may not be equipped to assess the level of risk in the cyber security products they are putting trust in. UNSW is in favour of enforcing more rigorous cyber security standards and practices such as the Essential Eight, however notes that this may only be achieved alongside a campaign to promote greater cyber awareness and resourcing within organisations.

At a bare minimum, there should be a basic standard for industry to comply with, that includes accountability measures for reckless behaviour that increases risks to other parties. In particular, developers and vendors of both hardware and software should bear greater responsibility for the products they have developed, as end users currently have to endure the consequences and responsibility for any defects.

UNSW is broadly supportive of better regulation and transparency of cyber security products and suggests that this could be achieved with a ratings system to inform customers about cyber security products.

Addressing the cyber skills shortage

If Australia is to meet the challenge of cyber threats, it is critical that as a nation we are adequately skilled to do so. The cyber skills shortage in Australia is well-known, but not well-understood. Substantial underinvestment by Government in cyber security in comparison to other countries has failed to produce the workforce needed now and in the future. An increase to funding for education measures is essential to ensure the skills shortage is addressed, even if the education measures funded are only simple.

UNSW recommends the Government develop a Cyber Workforce Strategy to identify cybersecurity workforce needs. The Cyber Workforce Strategy should seek to expand the cyber security workforce through greater investment in education and training and implement innovative strategies to recruit and retain skilled talent.

UNSW is a leading provider of cyber security education, offering cutting-edge technical courses as well as ones that are designed to produce well-rounded cyber graduates skilled in strategy, ethics and diplomacy. UNSW also offers a range of professional education courses catering to industry professionals. As our expertise in the field has demonstrated, the best education combines theory with integrated, practical learning. Consideration should be given to how the law interacts with cyber security education, to ensure that educators do not unintentionally commit an offense while conducting training activities.

As well as education, the other way to improve cyber resilience is to improve general community awareness around cyber risks, and easy actions to protect or mitigate against those risks. This is particularly the case with everyday consumer items that are increasingly becoming a risk, such as smart phones, smart speakers, and other interconnected appliances. UNSW acknowledges the work of the ACSC towards this end, but nevertheless recommends that a broader public awareness campaign would be beneficial, in combination with specific warnings relating to risky products. Consideration should be given to initiatives such as product labeling requirements, standards, warnings (for example, product ratings using a star system as occurs with energy efficiency) and enforcement of these rule by the Australian Competition and Consumer Commission (ACCC).

Conclusion

UNSW understands and supports the Government's desire to protect Australia's national interests from cyber security threats. Implementing better consumer protections and establishing standard industry risk management practices will go a long way towards improving cyber resilience in the community. Strategic investment in cyber security education is the only way to address workforce skills shortages needed to support the Government's cyber security agenda, and universities such as

UNSW are well-placed to deliver cutting-edge cyber courses that create world-class professionals. However, it is critical that the roles and responsibilities of government, industry, universities and consumers are well defined and understood.

We would be pleased to further discuss any issue raised in this submission. To do so, please contact our Senior Government Relations Officer, Tamara Lions on (02) [redacted] UNSW looks forward to working with you on this important matter.

Sincerely

[redacted]

Robin Schuck
Head of Government Relations
UNSW