UNIVERSITY OF
CANBERRA

Mr Andrew Penn
Chair, Expert Advisory Board
Australian Cyber Security Strategy
Department of Home Affairs

via: auscyberstrategy@homeaffairs.gov.au

21 April 2023

Dear Andrew,

Re: Development of 2023-2030 Australian Cyber Security Strategy

University of Canberra welcomes consultation on a *2023-2030 Australian Cyber Security Strategy* and is keen to participate.

We refer to the discussion paper and information on your website and are pleased to provide a submission to the panel.

The University of Canberra is well placed to comment on cyber security.

We have a partnership with global technology company Cisco, focusing on boosting Australia's cybersecurity resilience.

This partnership is assisting to address the national cybersecurity skills shortage, secure Australia's critical infrastructure, and expand the National Industry Innovation Network (NIIN), an alliance of companies and universities focused on the role that digital adoption can play in meeting Australia's economic and social challenges.

Attached is our submission prepared in conjunction with Mr Craig Mutton our Chief Digital Officer and Vice-President, Digital. We would be happy to discuss our submission with you at any time.

Yours sincerely,

[redacted]

Professor Paddy Nixon

Vice-Chancellor and President

E [redacted]

W www.canberra.edu.au

UNIVERSITY OF CANBERRA

2023 – 2030 Australian Cyber Security Strategy

University of Canberra Submission

April 2023

University of Canberra welcomes consultation on a *2023-2030 Australian Cyber Security Strategy* and is keen to participate.

We note the appointment of an Expert Advisory Board to lead this process and the appointment of a Global Advisory Panel to ensure the Strategy aligns with international best practice.

We refer to the discussion paper and information on your website and are pleased to provide a submission to the panel. This has been prepared in conjunction with Mr Craig Mutton our Chief Digital Officer and Vice-President, Digital.

The University of Canberra is well placed to comment on cyber security, and we are currently undergoing work to refine our own strategy in this area.

On 19 October 2022, the University announced its partnership with global technology company Cisco, focusing on boosting Australia's cybersecurity resilience. The partnership includes:

- The establishment of Innovation Central Canberra - a hub for industry and government to validate cybersecurity technologies, develop prototypes and de-risk the adoption process. The innovation centre is the sixth in a national network of Cisco innovation centres co-located on university campuses.
- The creation of a joint Research Chair in Critical Infrastructure and Defence. The Chair position will focus on applied research related to cybersecurity across several industries including Defence.
- Expansion of Cisco's Networking Academy to the University of Canberra, which provides learning curricula for careers in technology, including cybersecurity.

The partnership is assisting to address the national cybersecurity skills shortage, secure Australia's critical infrastructure, and expand the National Industry Innovation Network (NIIN), an alliance of companies and universities focused on the role that digital adoption can play in meeting Australia's economic and social challenges.

The University is a member of the Council of Australasian University Directors of Information Technology (CAUDIT). We have had input into CAUDIT's joint submission through the Australasian Higher Education Cybersecurity Service (AHECS) and support the general recommendations presented to the Advisory Board.

We are acutely aware of our responsibilities under the *Security of Critical Infrastructure Act 2018* and the extent to which parts of the University may be considered a critical education asset. In understanding this, we engage with the Cyber and Infrastructure Security Centre within the Department of Home Affairs.

More broadly we are aware of the security risks that international connectivity brings and the potential failure points that exist across the spectrum of university activities. We comply with our obligations under the *Foreign Influence Transparency Scheme Act 2018 (FITS Act)*, *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*, and the *Defence Trade Controls Act 2012*.

The University is pleased to work with the Universities Foreign Interference Taskforce (UFIT) and the Department of Home Affairs, particularly around the *Guidelines to Counter Foreign Interference in the Australian University Sector*. As a general principle, Government working collaboratively with universities to understand and mitigate risk is a preferred approach.

In this submission we present comments against selected questions that appear in Attachment A of the *Cyber Security Strategy Discussion Paper*.

Responses to select *Cyber Security Strategy Discussion Paper* questions

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

- Invest in Cybersecurity education and awareness campaigns (at all levels)
- Invest in Cybersecurity research and development
- Enhance International cooperation (R&D, education)
- Increased investment in cybersecurity infrastructure
- Foster a strong Cybersecurity and awareness culture
- Encourage partnerships between industry-academia, public-private

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

The University agrees that streamlining the regulatory frameworks would be useful. This might include further reform to the *Security of Critical Infrastructure Act*.

Given the increase in obligations and standards, it would be beneficial for Government to provide a straightforward pathway for compliance. A new Cyber Security Act could be a good mechanism to achieve this, but once such an Act is in place the Commonwealth would need to actively ensure that the agreed framework remains fit for purpose. Maintaining flexibility to respond to new challenges quickly and effectively is imperative, as is the ability to consider all aspects of any given scenario.

We recommend the Government pursues reform around privacy of information, including the right to privacy and the right to have personal data removed from systems. Information privacy needs to be more heavily enforced and should be a part of all process and integral to culture change. The Optus and Medicare breaches were exacerbated by the volume of historical data not previously disposed of. Any organisation which collects personally identifiable information should know their requirements and held accountable to meeting them, including any requirements for destruction.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

The University strongly recommends that Government ensures Australia's researchers are supported to develop and continue their international partnerships in cyber security and related disciplines. Australia needs sovereign capability, but it also needs to be strongly networked into the region and more widely, given the borderless nature of much cyber-crime and other unwelcome cyber activity. Through the work of university academics, including those at University of Canberra, Australia already has good international relationships and networks. These need to be nurtured through dedicated funding, that allows for small, medium, and large collaborations, ensuring Australia both contributes to and benefits from international efforts.

Our collaboration with Cisco is one example of a university / industry partnership that will boost Australia's cybersecurity resilience through a multifaceted collaboration.

7. What can government do to improve information sharing with industry on cyber threats?

Government sharing as much information as possible will enhance how industry prepares and responds to cyber threats. The sharing of information about attacks and responses between universities in the Australian university sector has been valuable in developing individual institutional mitigation plans and responses. Further improvements could be made as follows

- Continue to foster a culture of trust between industry and government agencies
- The introduction of various Government strategies to encourage information sharing (e.g., through incentivising, access to grants)
- Government must share threat intelligence appropriately with industry
- Develop clear guidelines for information sharing and transparency of the information

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

The requirements around notifiable incidents should be expanded to ensure all organisations notify affected users when their data has been significantly compromised. It is essential to allow for a proportionate response to a breach, with consideration given to the seriousness of the breach as well as reputational damage to the organisation.

Making more information available would improve public understanding and assist in providing opportunities for extending collaboration. The stigma of being the subject of a cyber security incident should be addressed, and sharing of this information could be used to encourage engagement on the issues. Open collaboration is not possible when details of cyber security incidents remain secretive.

10. What best practice models are available for automated threat-blocking at scale?

The University encourages a balance of models. Ensuring that there is an appropriate balance of regulation, information and support is critical to the success of a whole-of-country approach. With particular regard to the Telecommunications Act, we suggest guidelines and incentives for telecommunications providers to address threat-blocking would be an appropriate improvement.

While 'industry' is discussed in this paper, there is a wide range of non-profit and community organisations which may not fall in this category. It is appropriate these are considered with regard to Australia's approach to cyber security, and possibly being included in formal compliance frameworks.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Yes. University of Canberra believes that given the ongoing need for both a dedicated workforce and a more general uplift of cyber skills amongst all age groups, a tailored approach is appropriate.

A great example of this is our partnership with Cisco.

Within Australia, Cisco has created the National Industry Innovation Network (NIIN). The NIIN is an alliance between industry and universities driven by one goal; to realise digital opportunities that can benefit the lives of all Australians.

The NIIN is working on nationally significant projects, including, securing critical infrastructure, education, digital health, and hybrid work environments through a range of initiatives:

- Partnerships
- Research Chairs
- Innovation Central
- Specialised Centres
- Skill & Talent Development

Partnerships are at the heart of the NIIN. Both industry and universities pool assets and expertise, including research, administration, IT and teaching, all with matched funding commitments. The current National Industry Innovation Network consists of partner Universities across five capital cities, each specialising in a specific industry sector. The Canberra node focusses on Defence, Cybersecurity and Infrastructure.

University of Canberra's partnership with Cisco Networking Academy also includes short courses and professional training through in Networking, Programming, Internet of Things (IoT), and Cybersecurity.

A tailored approach might include

- Government funded cadetships, internships, apprenticeships
- Industry certifications and training programs
- Awareness campaigns
- Hackathons, Cybersecurity competitions
- Govt-industry partnerships

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

The University calls on the Government to recognise cyber security as a national priority both now and for the future. Support in education includes continued funding for teaching, research and infrastructure in universities as it pertains to cybersecurity and digital more broadly.

We recommend the Government continue to support and incentivise industry partnerships. Fostering partnerships between industry and universities can create opportunities for research and development of new cyber security technologies and strategies, as well as creating opportunities for industry-led training and education programs.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Yes, we would support a streamlined method. If Australia is to have a whole-of-nation approach, and the capacity to learn from cyber incidents, then a streamlined approach would be helpful.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Assisting bodies would benefit from greater power and reach. ASD/ACSC should be a centralised hub of assistance and guidance for all levels of business, industry, and government. These bodies should be able to provide timely assistance in the case of cyber incident to companies, including a guidance service delivering expert and current advice. These capabilities are currently distributed across private industry which is unaffordable for many smaller business.

Building on the reputation of ACSC/JCSC, greater collaboration and benefits for assistance service and information sharing could be achieved.

17. How should we approach future proofing for cyber security technologies out to 2030?

- Through a risk-based approach through identification and prioritisation based on their potential impact to the organisation
- Embracing and investing on emerging technologies: Web3, blockchain, etc.
- Invest in research and development between academia and industry.

20. How should government measure its impact in uplifting national cyber resilience?

- Benchmarking through international standards, such as the Cybersecurity Framework developed by the US National Institute of Standards and Technology (NIST)
- Establish clear metrics for implementing Cybersecurity best practices
- Regular assessments, auditing and reporting

University of Canberra

The University is incorporated under the University of Canberra Act 1989 of the Australian Capital Territory.

We are committed to serving the people of Canberra and the region through professional education and applied research.

University of Canberra is ranked among top universities globally by both Times Higher Education (THE) and QS World University Rankings and appears in the 2020 THE rankings as one of the top 300 universities in the world and one of the top 20 young universities under the age of 50 years.

The University has released *Connected*, a decadal strategy that sets out the long-term ambitions and objectives for our university. It has at its core explicit commitment to our staff and students, to our place in Canberra and the region, and to the Ngunnawal people.

Our ambition for the coming 10 years is to be a global leader in driving equality of opportunity. A commitment that ensures we are the most accessible university in Australia; building an international identity for University of Canberra that celebrates, and is built upon, the importance of our place, one of national and international decision making. We proudly embrace our role as the university of the nation’s capital.

The University of Canberra has had long-standing excellence in both teaching and mission-oriented problem-solving research and continues to be influential in a range of areas including health and wellbeing, nursing, education, information technology, communications, architecture and design, sport, and science.