CAUDIT
Council of Australasian University Directors of Information Technology

Strengthening Australia's cyber security regulations and incentives

CAUDIT Response
August 2021

The Council of Australasian University Directors of Information Technology (CAUDIT), with input from its members, submits the following response to the Department of Home Affairs on the consultation on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy.

CAUDIT is the peak member association supporting the use of information technology and cyber technology in the higher education and research sector in Australasia. CAUDIT is a registered Not-For-Profit Association with 63 members including all public universities in Australia and New Zealand along with those of Papua New Guinea and Fiji plus key national research organisations in Australia. Members are represented by the most senior person with strategic responsibility for Information Technology (IT) operations and digital transformation in their institution i.e., the CIOs, CDOs and IT Directors of each member organisation.

CAUDIT is leading the Australasian Higher Education Cybersecurity Service (AHECS) was formed in 2019 as a CAUDIT initiative and is delivered in collaboration with Australia's Academic and Research Network (AARNet), AusCERT, Research and Education Advanced Network New Zealand (REANNZ) and the Australian Access Federation (AAF). This was as a result of the CAUDIT Member Representatives (CIOs of institutions) voting cybersecurity being voted as their number one priority for collective action in 2018.

AHECS supports the ability of universities to continue to operate in the face of cyber challenges, aiming for minimal negative impact on their stakeholders (students, staff, third parties – other universities, government, industry), teaching and learning and research. This is being achieved through coordination of the substantial human assets of members and partners to inform direction, advocate, share intelligence, reduce barriers to the implementation of good practice, identify and act on capability gaps, and holistically defend the sector from continuously evolving Cyber Security threats in conjunction with key vendors. AHECS aligns with and supports the University Foreign Interference Taskforce (UFIT) cybersecurity goals.

This is an active initiative with AHECS' goals covering a range of collaborative activities, in a trusted environment, aligned with the principles of being stronger together and 'all boats lift on a rising tide'. It is a service by the sector, for the sector.

CAUDIT and the AHECS partners are ready and well placed to support Government cybersecurity initiatives and proactively help the Higher Education and Research sectors in ensuring the national security risks affecting the Australian higher education and research sector are appropriately managed and addressed.

CAUDIT welcomes the opportunity to comment on the consultation on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy. CAUDIT strongly supports addressing the evolving threats to national security and improving cyber resilience of the sector.

CAUDIT's response to the Strengthening Australia's cyber security regulations and incentives provides the following key recommendations.

1. Governance standards for large businesses.

The management of cybersecurity risk is important in addressing the maturity of large businesses and their capability to address the threat landscape. The adversaries we are fighting are increasingly sophisticated, well-resourced, and constantly changing. As identified in the paper, there are 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses. Universities will be covered by the Security Legislation Amendment (Critical Infrastructure) Bill 2020 as well as potentially being covered as large business under any legislation flowing from the consultation on Strengthening Australia's cyber security regulations and incentives.

Regulatory frameworks are an important basis for managing cyber security in Australia. However, in the context of 51 laws that form some form of cybersecurity obligation on businesses, this should be appropriate to risk and harmonious across government to support responding to the threats, rather than regulatory requirements. The University Foreign Interference Taskforce (UFIT) guidelines are recommended as the appropriate means for addressing cybersecurity threats in the higher education context.

Recommendation: The Government provide a framework for coordination of all government security-related agendas, ensuring harmonising of legislation and relevant industry-based standards.

Recommendation: Continue to strengthen consultation with the sector and recognised vehicles for this including the University Foreign Interference Taskforce (UFIT), Universities Australia, AHECS and CAUDIT.

2. Responsible disclosure policies

The responsible vulnerability disclosures being incorporated into regulatory frameworks to increase adoption of good practices is strongly encouraged. It is acknowledged that this would create a regulatory burden, however, this is offset by the benefits from addressing the vulnerabilities. With the regulatory burden it will create a momentum to address vulnerabilities and provide protection to those reporting the vulnerability.

Vulnerabilities should not be limited to software. The consultation paper switches between vulnerabilities, software vulnerabilities and vulnerabilities in software and systems. A clear single definition of vulnerabilities to include all vulnerabilities that have the potential to compromise integrity, availability or confidentiality of digital information should be documented.

Recommendation: Enact a regulatory framework to address vulnerability disclosure including clear definition of vulnerabilities addressed with the regulatory framework.

3. Set clear minimum expectations, increase transparency and protecting consumers

The goals on setting clear minimum expectations, increasing transparency, and protecting consumers are welcome additions to addressing the risks faced by small business and consumers. The threats can be daunting for small business and consumers with the portrayal of hoodie wearing threat actors. It is recommended to provide practical guides to support the standards to assist in providing the tools that support translating these standards into real, actionable outcomes that address the risk.

Recommendation: Provide practical guides to support clear standards in addressing the elements that address small business and consumers to increase adoption.

Thank you for the opportunity to provide feedback on Strengthening Australia's cyber security regulations and incentives. The initiative is another important step forward in providing measures to provide meaningful action in addressing the increasing threat landscape.

If you would like further information or to explore any of these comments, please contact:

Jenny Beresford
Chief Executive Officer
Council of Australasian University Directors of Information Technology (CAUDIT)
[redacted]