CAUDIT
Council of Australasian University Directors of Information Technology

**Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018**

The Council of Australasian University Directors of Information Technology (CAUDIT), with input from its members, submits the following response to the Parliamentary Joint Committee on Intelligence and Security review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

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 institutions in Australia. Member Representatives are the most senior person with responsibility for Information Technology (IT) operations and digital transformation in their institution i.e. the CIO, CDO or IT Director of each member institution.

CAUDIT members prioritised cybersecurity in 2018 as the number one initiative for CAUDIT to address in collective action for the Higher Education sector. In response CAUDIT, partnering with Australia's Academic and Research Network (AARNet), AusCERT, Research and Education Advanced Network New Zealand (REANNZ) and the Australian Access Federation (AAF), has established the Australasian Higher Education Cybersecurity Service (AHECS).

AHECS is supporting the ability of universities to continue to operate in the face of cyber disruptions, aiming for minimal negative impact on their stakeholders (students, staff, third parties – other universities, government, industry) and teaching and research. This is being achieved through coordination of the substantial human assets of the higher education sector 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.

By having this coordinated approach, built on an established framework (NIST) and backed by delivery of key services and advice, we can collectively more easily support the cyber resilience of individual institutions and the sector, protect university assets and the personal information of students and staff. Through AHECS, CAUDIT, AusCERT, AARNet, REANNZ and AAF we will deliver services targeted at higher education in four areas: engagement, advocacy and advice, support and operations, and training.

AHECS partners are ready and well placed to support the Government and proactively help the Higher Education and Research sectors in ensuring the development of our nation's Protecting Critical Infrastructure and Systems of National Significance and commitment to protecting Australians from cyber threats.

PO Box 9432, Deakin ACT 2600 | ABN 39 514 469 351
Phone: +61 2 6222 7575 | Email: caudit@caudit.edu.au
www.caudit.edu.au

CAUDIT
Council of Australasian University Directors of Information Technology

CAUDIT welcomes the opportunity to comment on the Parliamentary Joint Committee on Intelligence and Security review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020. CAUDIT, with input from its members, has responded to the Department of Home Affairs consultation paper on Protecting Critical Infrastructure and Systems of National Significance and the Exposure Draft Bill of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill).

CAUDIT welcomes the additional opportunity to reiterate the support and concerns on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to the Parliamentary Joint Committee on Intelligence and Security review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020. CAUDIT has welcomed the Government's approach and stated intention to co-design and consult with the sector on this, related legislation and implementation. The sector concerns provided on the Department of Home Affairs consultation paper on Protecting Critical Infrastructure and Systems of National Significance and the Exposure Draft Bill of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) still remain following the introduction of the Bill.

The Bill, as presented, has not significantly expanded on the consultation paper or Exposure Draft Bill.

CAUDIT's response to the Bill identifies the following key recommendations.

1. **No one size fits all model**. Protecting critical infrastructure is important, however, within education, research and innovation, there is no 'one size fits all' model for universities. To apply that approach risks implementing security obligations suited to those aimed at high risk research-intensive defence-aligned institutions to all and hence applying too high an obligation on teaching-focused and dual-sector institutions. The scale, complexity and threat landscape are different from university to university. It is important to also provide guidance on principles for potential inclusion of private research institutions such as CRC spinoffs. The model must support a risks-based approach to critical infrastructure supported with clear boundaries between the responsibilities of federal and state governments, regulators, and entities. A narrowing of scope in relation to universities may be beneficial to successful implementation within the higher education sector.

   **Recommendation: Apply a targeted, risk-based model proportionate to critical assets held and reflective of institutions' risks.**

2. **Definitions**. Clear definitions are vital to effective implementation. 'Critical infrastructure', 'education asset', 'incident' and 'systems of national significance' need to be clearly defined. Definitions are clarified through consultation will assist in understanding; or example the definition of what constitutes a 'mandatory incident' along with the 'reporting timeframe' for incident types.

   **Recommendation: Work with the sector to more clearly define key elements such as education asset, incident and systems of national significance applicable to education and research.**

3. **Consultation**. The current proposal provides for consultation in detail post implementation of the legislation. Implementation has aggressive timeframes followed by unclear timeframes for meeting the legislative requirements. It will assist if the phases and "switch on" timing of components of the legislation are clearly defined and identified through consultation. As an example, the 12- or 24-hour window to report incidents may not allow sufficient time to understand the incident to enable meaningful reporting. The GDPR legislatively implemented standard reporting requirement is 72 hours.

 PO Box 9432, Deakin ACT 2600 | ABN 39 514 469 351
Phone: +61 2 8079 2533 | Email: caudit@caudit.edu.au
www.caudit.edu.au

CAUDIT
Council of Australasian University Directors of Information Technology

**Recommendation: Agree, through consultation with the sector, the legislation details, definitions, standards, and implementation timeframe.**

**Recommendation: Consult on appropriate time to adapt to requirements.**

4. **Incentivise cyber**. Cyber defence and offence needs investment and through prudent Government investment Australia can continue to build a global cyber industry. This will provide export opportunities, a vibrant life-long education environment where talent is developed and incentivised to remain in Australia and support regional communities while ensuring funding to universities is proportional to the challenge in protecting national assets. Universities are financially challenged at present; and will face financial challenges at least through to 2024 as the sector recovers from the impacts of the COVID-19 pandemic. The goals of this legislation can be achieved through the government adopting a phased approach in order to 'right-size' solutions proportionate to the risk and providing support and platforms to assist with compliance. Consideration and support for sector initiatives such as the Australasian Higher Education Cybersecurity Service (AHECS) (which includes the AARNet SOC) along with support from government will ensure coordinated responses and effective sector risk mitigation.

**Recommendation: The Government incentivise investment in cyber across the sector to underpin cybersecurity obligations in addressing the evolving challenges while broadening the ecosystem and education underpinning cyber security.**

5. **Harmonious legislation and standards**. The adversaries we are fighting are increasingly sophisticated, well-resourced, and constantly changing. Universities and businesses can no longer go it alone and only through strength in unity, scale and efficiency do we have a chance to mature the Australian cybersecurity landscape to address the challenges. The many underpinning legislation and standards, such as University Foreign Interference Taskforce (UFIT) guidelines, Privacy Act Notifiable Data Breaches scheme, a National Security Standard, and the Draft Bill of the Security Legislation Amendment (Critical Infrastructure) Bill 2020, along with responses such as AHECS and the 'Enhancing Cyber Security Across Australia's University Sector' project managed by University Foreign Interference Taskforce (UFIT) need to be progressed with full visibility, appropriate to risk and harmonious across government to support responding to the threats.

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

Thank you for the opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

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

Anne Kealley
Chief Executive Officer
Council of Australian University Directors of Information Technology (CAUDIT)
[redacted]