CAUDIT
Council of Australasian University Directors of Information Technology

Protecting Critical Infrastructure and Systems of National Significance

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 consultation paper on Protecting Critical Infrastructure and Systems of National Significance.

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 universities in Australia and New Zealand along with those of Papua New Guinea, Fiji and Timor-Leste plus key national research institutions in Australia. Member Representatives are the most senior person leading Information Technology (IT) operations in their institution i.e. the CIOs, CDOs and IT Directors 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

This submission is the product of an open call for expressions of interest from CAUDIT's membership to participate in a working group to respond to the consultation paper on Protecting Critical Infrastructure and Systems of National Significance and correlate the member feedback. Working group membership:

Position	Name	Title	Institution
Chair	Anne Kealley	Chief Executive Officer	CAUDIT
Member	Greg Sawyer	Strategic Initiative Development Manager	CAUDIT
Member	Joshua Qwek	Cybersecurity Architect	The University of Western Australia
Member	Fadi al Jafari	Information Security & Risk Manager	Deakin University
Member	Mardi Griffiths	CISO	Swinburne University
Member	David Stockdale	Deputy Director, ITS & Director, AusCERT	The University of Queensland

Thank you for the opportunity to respond to consultation paper on Protecting Critical Infrastructure and Systems of National Significance.

CAUDIT's response to the call for views identified the following key recommendations.

1. **Harminious legislation and standards**. The adversaries we are fighting are increasingly sophisticated, well-resourced and constantly changing. As with the new Australasian Higher Education Cybersecurity Service (AHECS) initiatives, institutions 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 need to be coordinated, appropriate to the risk and harmonious across government to support responding to the threats.

   Recommendation: The Government provide a framework for coordination of all government agencies, ensure harmonious legislation and relevant industry based standards.

2. **No one size fits all model**. Within education, research and innovation, there is no one size fits all model for institutions. To apply that approach risks reducing security obligations to high risk research intensive defence aligned institutions or applying too high an obligation on regional teaching focused institutions. The scale, complexity, capability and threat landscape are different from university to university. The models must support a risks-based approach to critical infrastructure.

   Recommendation: Apply a risk based model reflective of institutions risk.

3. **Incentivise cyber**. Cyber defence and offence needs investment and through prudent Government investment Australia can build a global cyber industry providing export opportunities, a vibrant life-long education environment where talent is developed and incentivised to remain in Australia and support regional communities and ensure funding to universities, agencies, like AustCyber and ACSC, is proportional to the challenge in supporting developing the ecosystem.

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

4. **Disclosure protection**. Currently, Australia does not have protection for responsible disclosure. The legislation will provide a positive cybersecurity obligation on institutions but there is no coordinated approach to disclosure protection.

   Recommendation: The Government provide disclosure protection to support rectifying deficiencies in critical infrastructure.

5. **Broaden definition of critical infrastructure.** The definition of critical infrastructure reflects on the physical aspects of critical infrastructure. At the same time, it is important to incorporate the tangible elements that underpin the "infrastructure". In Education and Research the people assets, teaching, research relationships and partnerships can be more critical, or at least of equal critcality, as the physical assets.

   Recommendation: The Government broaden the definition to include the people element.

CAUDIT, with input from its members, provides the following responses to the 36 questions laid out in the consultation paper:

View	Call for view	Response
1	Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?	In relation to Education, research and innovation, yes these functions are vital to Australia's economy, security and sovereignty. Each sector within this definition requires appropriate risk based treatments specific to the sector and defined risk. The definitions of Education, research and innovation need to be defined providing proportionate to the risk. The risk for a teaching university compared to a defence intensive research university are different, as it is to a dual sector institutions.
2	Do you think current definition of Critical Infrastructure is still fit for purpose?	The term infrastructure implies a physical assets . The current definition is asset focused and fails to capture the human capital in the equation. While for telecommunications this may be critical, within education and research the people element is the critical element. The wording should be reviewed to incorporate the tangible elements that underpin the "infrastructure". In Education and research the people assets, teaching, research relationships and partnerships would be more critical, or at least of equal criticality, as the physical assets. The processes requires the rigor to allow for progression to higher and lower risks, as organisation change to address the marketplace. An example of this progression may be related to the award of a defence research project for increasing cybersecurity obligations and maturity, whereas completing a defence research project may decrease the obligations on that institutions. The underpinning governance is the cybersecurity obligations applied to an institution are appropriate to the risk profile and impact.
3	Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	The factors for consideration when identifying and prioritising critical entities and entity classes include: ▪ Immediate and long-term impact ▪ Breadth of organisation - all-encompassing versus spoke targeted on the risk ▪ Supply chain risk both as delivering and consuming ▪ Financial impact ▪ Capacity to achieve the obligations including resources in people and technology ▪ Complicating factors medical research, defence partnerships, state government, foreign investment

4	What are the common threats you routinely prepare for and those you have faced/ experienced as a business?	The common threats identified within the sector: phishing; ▪ spear phishing; ▪ preparing for ransomware, criminal activity; ▪ disruption to operations, reputation; ▪ impact on people (staff, students, alumni) ▪ Denial of service events, ▪ PII data breaches, ▪ Research data leak, ▪ financial fraud, ▪ distribution of misinformation, ▪ contract cheating
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	The lens for assessing the criticality requires a multi-dimensional filter to incorporate the factors to ensure the application is appropriate to the risk and impact, appropriate to the organisation and addresses the outcomes. The outcomes need to be tied back to the economy, the community, and Australia's sovereignty. The factors will include the intermediate and long-term impact completed against comparative mapping. An example would be definition tied to defence with unclassified resulting in limited risk and damage. This would progressively increase with classified tied to exceptionally grave damage applying appropriate risk controls and security obligations.
6	Which entities would you expect to be owners and operators of systems of national significance?	In relation to Education, research and innovation the institutions through the relevant institutional governance will be the owners and operators of systems, people and processes. Aligned to this will be the industry partners of the institutions. An underlying principle is that critical infrastructure should not be owned or controlled by foreign institutions.
7	How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	A revised Threat Intelligence Sharing Network (TISN) will be an integral component in assisting to meet the positive security obligations. The interactions through the JCSC/ ACSC forums have been of benefit. The Education, research and innovation sector needs to incorporate the work by sector leaders including AHECS, AusCERT and AARNet.

8	What might this new TISN model look like, and what entities should be included?	Education, research and innovation TISN will be sector coordinated and supported by government capitilising on the work underway in the sector including by AHECS providing cybersecurity coordination and services for the sector, AusCERT as Australia's pioneer cybers emergency response team and AARNet leading the sector Security Operations Centre (SOC) and National Research Education Network (NREN) threat intelligence sharing initiative with 5 eyes countries.
9	How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?	The government is recommended to establish centres of collaborations to support enhancing the sector capability remains a "team sport". The government could mandate and fund the centres to remove barriers to entry. Key components in the collaboration will include providing sector relevant documentation designed to be a baseline for institutions to enhance relevant to institutional risk profile while ensuring a sector baseline. Sector focused workshops to assist in the transition to meeting the security obligations providing clear and documented guidance for the sector to follow aligned to a sector agreed appropriate frameworks. The government should also ensure consistency across the government and departments in relations to regulations, standards and frameworks to support cohesive cybersecurity requirements. This will include Protecting Critical Infrastructure and Systems of National Importance, Foreign Interference and the University Foreign Interference Taskforce (UFIT), 2020 Cyber Security Strategy, Ensuring integrity in higher education, National Cybersecurity Standards and the Defence Industry Security Program (DISP).
10	Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	Yes.
11	Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	The security requirements are not adequately defined at this stage. For example, the standards that will be applied are expected to be developed through sector consultation and engagement. This questions should be re-issues following the documentation of how the legislation will apply and the underlying standards, controls and obligations.

12	Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?	The institutions are operating in line with the principles but have varying levels of maturity across the sector. Depending on the details of the legislation and underpinning documentation, will depend on the time required to meet the security obligations. How the definition is applied will also determine the time and cost. For example, requiring the same positive security obligations against an existing defence integrated research institution compared to a regional teaching focused institution has the potential to either water down the obligations so that all institutions can meet or raise the requirements inappropriately to the risk for smaller institutions who will be negatively impacted, and potentially financially unable to meet the obligations.
13	What costs would organisations take on to meet these new obligations?	The sector needs to understand the expected security baselines in order to assess the uplift required. As it stands, all institutions will be covered under a broad brush approach of require a positive security obligations. The sector does not support this approach, partly because of the cost impact to many of the institutions who do not have the risk profile to justify the obligations. The sector as a whole has been negatively impacted by the impacts of COVID and will be financially challenged in responding to the potential of increased costs. At this stage, the costs are expected to be related to enhancing the various portfolios within institutions to address the gaps. Both of these elements will mandate appropriate time to review, evaluate and address the obligations.
14	Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?	Institutions do have state based legislative standards that vary from state to state. The main cost involves updating the governance process based on the changes.
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	There is potential that it will create duplication and overlap if this is not harmonious with other government initiatives including Foreign Interference and the University Foreign Interference Taskforce (UFIT), 2020 Cyber Security Strategy, Ensuring integrity in higher education, National Cybersecurity Standards and the Defence Industry Security Program (DISP).

16	The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	The regulator needs to have clearly defined objectives that are well communicated to the sector. This should include a period where the main objective is to assist and advise rather than regulate. The principles of measuring compliance against those guidelines should be as clear as possible. To assist institutions in progressing their obligations, a list of qualified and experienced third parties to provide guidance and expertise will assist. The sector regulator perform audits and if these are outsourced to third-party audit providers compliance with documented secure mechanisms to gather evidence and mask sensitive information is required.
17	Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	No response
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	No response
19	How can Government better support critical infrastructure in managing their security risks?	The government can better support critical infrastructure at a sector level through funding well defined initiatives aligned to critical infrastructure outcomes with preference given to sector wide and sector delivered initiatives. There is an opportunity to review Board and executives having duties similar to current ASIC organisations responsibilities. Those duties mean board and executives are accountable for any cyber incident that impacts the general public or causes significant unrecoverable losses.

20	In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?	The breadth of higher education and research means that a single model is impractical. Research in scram jets or quantum computing needs different controls to English literature. The use of schemes such as DISP in other key research areas is one way forward.
21	Do you have any other comments you would like to make regarding the PSO?	As per previous comments what are the baselines protections for HE. Without knowing this it's hard to comment further on appropriateness. How is the Gov determining the tier levels (e.g. gov assistance, ECSO or PSO)? Will parts of an institution be considered top tier (PSO) and other parts have lower tier levels?
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	Established and adopt a "Common Information Model" to ensure that we are all on the same baseline for information. This would be underpinned by declassifying information quickly so as to disseminate in a timely manner and reviewing adoption of an early warning system to actively notify organisations coordinated through ASD/ ACSC.
23	What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?	Through ASD/ ACSC provide dedicated sector liaison to continue to provide opportunities to brief and raise awareness on the real life threat landscape and the lessons learnt.
24	What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?	The sector, institutions and AHECS Partners CAUDIT, AusCERT, AARNet, REANNZ and AAF possess a significant amount of data and information on the threat picture. There is an opportunity, as with the CAUDIT ISAC delivered by AusCERT and AARNet SOC to capitilise collectively on the availability to address known threats, share data and detail the impact of breaches. There would be potential cost implications involved in developing the model, resourcing the solution and supporting the outcome. The AHECS Partners are well placed to provide elements of or the solution.

25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	There are a number of techniques to identify the vulnerabilities at the perimeter of critical networks. Continue with the scanning ASCS performs including reviewing in the post pandemic architecture the inclusing the SaaS and cloud services. Review sector aggregation of services, potentially through AUsCERT and AARNet, to provide baseline and advanced capability that can integrate into institutional capabilities.
26	What are the barriers to owners and operators acting on information alerts from Government?	The maturity across the sector varies, as does the impact of the information alerts. Resourcing and consistency of intrepretation of the risk and alerts will play a part in the response.
27	What information would you like to see included in playbooks? Are there any barriers to codeveloping playbooks with Government?	There are no barriers to codeveloping playbooks. This approach would be encouraged to provide scale and efficiency across the sector. Playbooks could include: ▪ Communication and engagement models ▪ Escalation paths with transparenct into subsequent actions ▪ Cross-entities that identify when/ how peers across industry can be engaged
28	What safeguards or assurances would you expect to see for information provided to Government?	The treatement should adhere to the traffic light protocol (TLP) as an existing standardised safeguards for treating information. In regards to compliance to the legislation, unified dashboards with clear metrics that organisations can follow and self-assess against.
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	The government exercising direct action should be used only for an extreme risk. At the individual organisation level, it should have approval of the chief executive, for example the Vice Chancellor. Where an institution is unable to respond directly to a threat and requests assistance, the government should cooperatively provide the assistance where this relates to the national interest. This will require the establishment of cooperative force to respond to those situations involving representatives from multiple sectors in this force.

30	Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?	In response to reception of the declatation, at the individual orgisation level, it should have approval of chief executive, for example the Vice Chancellor. For any institution covered by the declaration, information pertaining to declaration should be provided and as applicable, be updated as the emergency progresses. In short, the government must be transparent with affected institutions and as far as possible, with the sector to mitigate potential future risk. In response to who should have the power to declare, this is a government responsibility to ensure that an appropriately informed and empowered role maintains this responsibility and exercises it with due caution. The ability to enact the resourcing the declaration of an emergency is a pre-requisite for the role.
31	Who should oversee the Government's use of these powers?	The Office of the Audit General providing accountability by reporting independently to Parliament and entities.
32	If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?	This is a question for government as only government and its agencies will have the most complete understanding of the threat and political landscape. The actions must tie to the outcomes of the legistation in protecting critical infrastructure.
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	Like the Privacy Act, it is recommended to clearly identify who in the organisation are ultimately liable and what are the consequences both at a personal and organisation level. Within governement, the agencies should be legally empowered to provide offensive and defensive capability to protect Australia's critical infrastructure with this framework.
34	What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?	No response
35	What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?	No response

36	Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?	At this stage in the process, the definitions and standards are unclear in response to the obligations and assistance required. Further consultation is recommended when the detailed legislation is updated to ensure the response is specific to regulation, not perception of how it may or may not be applied.

Thank you for the opportunity to provide feedback to the consultation paper.

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]
[redacted]