AUSTRALASIAN HIGHER EDUCATION
CYBERSECURITY SERVICE **(AHECS)**

2023–2030 Australian Cyber Security Strategy: Legislative Reforms

Australasian Higher Education Cybersecurity Service (AHECS) submission

Classification: Public

24 February 2024

The Australasian Higher Education Cybersecurity Service (AHECS) is the higher education and research sector's peak cybersecurity body. AHECS represents the sector on cybersecurity issues, leveraging the capabilities and expertise of its partner entities to strengthen the overall cybersecurity posture of the sector.

AHECS is delivered in collaboration with Australia's Academic and Research Network (AARNet), AusCERT, Council of Australasian University Directors of Information Technology (CAUDIT), Research and Education Advanced Network New Zealand (REANNZ), and the Australian Access Federation (AAF). This collaboration illustrates a joint approach by higher education institutes and key supply chain partners including the sector's internet service providers (both Australian and New Zealand), federation provider, and cyber emergency response team.

AHECS purpose is aligned with the principles of being stronger together and 'all boats lift on a rising tide'. AHECS was developed specifically for the sector by the sector, to collectively mature the sector's capabilities, and continuously evolve and strengthen cybersecurity defences in the ever-changing environment of cybersecurity threats. This is achieved through the coordination 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 cybersecurity threats in conjunction with key vendors.

AHECS welcomes the opportunity to collaborate with the Australian Government on our nation's cyber legislative reforms. Please note, the views expressed in this submission result from contributions of many organisations (AHECS partners and CAUDIT Member Institutions), and, as such, may not represent the views of all participating organisations. Rather, they are reflective of the overall expertise and interests of the collective sector-based group. Each partner or member institution may provide their own individual submission, as appropriate.

A SECTOR PARTNERSHIP WITH AAF, AARNET, AUSCERT, CAUDIT AND REANNZ

After consultation with AHECS Partners and Members, AHECS makes the following general recommendations regarding the 2023–2030 Australian Cyber Security Strategy Legislative Reforms:

1. **Support**

   AHECS is supportive of the Australian Cyber Security Strategy. The strategy is well conceived and structured. The reforms are timely, progressive, and relevant to the Australian community. The strategy provides a targeted focus on multiple relevant fronts, but we encourage the government to undertake periodic review with independent engagement, consultation, and a willingness to realign the strategy in response to the rapidly changing environment. This process and the commitment to deliver upon this strategy should be transparent. We appreciate the focus on sovereignty and risk aligned actions. All of the legislative reforms should be informed by assessment of risks to individuals, organisations, the community and the nation and proportionate to the current and assessable future threat.

   Key recommendations

   - That the Government commit to periodic review of the Cyber Security Strategy.
   - Reforms and legislative changes should be aligned to an assessment of risks to individuals, organisations, the community, and the nation.

2. **Collective resourcing (within Government, industry, sector)**

   We are concerned that there may be a lack of sustainable support and insufficient collective resources to realise the reforms recommended in this strategy, as well as any subsequent legislative reforms. The strategy notes that resources will be needed to deliver the initiatives, especially as it related to small business. However, it appears that the intention is to allocate resources to strategy implementation and governance across government departments and agencies, rather than directly in industry. It doesn't address a need for sustained support or identify ways for government to partner with key sectors in industry. Government departments are currently under strain from existing legislative and standards requirements which adds challenges to individuals, industry, business, and the community to comply and be supported in a timely manner. The strategy has an opportunity to direct focus and funding to industry to develop national best practice which can then be applied more broadly across industry verticals in a trickle-down benefit approach. This also presents opportunities to develop the local security and risk supply chain. Given there is a globally recognised shortage of resources with relevant cybersecurity skills, the government should try and minimise introducing anything that requires additional effort without much risk reduction gain. For example, utilise existing communities of practice, and cross-sector intelligence platforms, and provide support to uplift these instead of attempting to reinvent and deliver from within government.

Key recommendations

- Consider resource requirements on future legislative reforms and to enact strategic activities, on a sustainable long-term basis.
- Understand the impact across the entire ecosystem and simplify to reduce the burden of compliance.
- Consider a principle of adaptation and reuse rather than overlaying reforms.
- Consider partnering with key industries to support a broader uplift.

3. Sustainability for independent and industry representation

AHECS supports impartial, transparent, and independent representation for the strategy implementation and legislative reforms. This should be in the form of a governance body that provides an independent perspective, with an ongoing remit, systemic input and sustained resourcing.

Key recommendations

- Consider sustained, impartial, transparent and independent representation.
- Clear remit and governance purpose should be established to support these legislative reforms appropriately.
- Conflict of interest should be independently assessed.

4. Responses to Discussion Paper questions

Part 1 – New cyber security legislation	
Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices	
1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?	The manufacturer and/or supplier (including resellers, and importers) of smart devices should be responsible for providing product that complies with the regional cyber security standards, akin to other product standard compliance (e.g. safety) within Australia. This is especially important in relation to devices aimed at consumers. We encourage the government to consider impact on competition, and on innovation, of limiting the availability of certain device classes to businesses or institutions. Software developers should also be responsible for software security standards compliance.
2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?	We believe that the government is in the best position to assess the appropriate standards and nominate minimum standards in alignment with risk to the national sovereignty and Australian community members. The first three principles should be the minimum, but not necessarily the whole.
3. What alternative standard, if any, should the Government consider?	As above, the government has oversight of the threat landscape and ongoing engagement with international counterparts, which put the

	government in the best position to nominate appropriate standards.
4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?	Adopting the definition used in the PSTI Act (UK) helps industry to standardise its approach across jurisdictions, providing cost efficiencies and likely improving security outcomes by encouraging a unified approach from manufacturers and enabling agencies across countries to collaborate on response. The PTSI Act presents a solid starting point.
5. What types of smart devices should not be covered by a mandatory cyber security standard?	We refer to the response to question 4.
6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?	The average lifecycle of smart devices is approximately 36 months. Twelve months warning for all ‘new’ devices, products, and services is a fair transition period. For existing products there should be an improvement in communication within 12 months (i.e., for how long will the software be updated, and an ability to receive reports on any vulnerabilities identified). A longer period will then be required to phase out the existing smart devices with a 36-month limit (unless they are supported for longer than this). Thus, an acceptable timeframe of maximum 36 months would allow for obsolescence and application of new requirements. However, the process should also be agile to allow for swift

	response to technical developments and emerging vulnerabilities.
7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?	The Government is best placed to determine this, after reviewing the landscape and conversing with international counterparts regarding experiences and lessons learned. The government will need to be very clear on how compliance will be monitored.
Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses	
8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?	While ransomware has business, financial and national impact, there are many more threats with as significant impact. The government should consider this in its approach, otherwise runs the risk of needing to undertake additional measures when the next significant threat challenges national sovereignty, businesses, and the Australian public. The benefit of ransomware incident reporting is in sharing meaningful, actionable, and timely information on the actor. Currently, actionable information is limited. Mandatory information for reporting should be minimal, especially in the early days of an attack when so much is unknown. Examples of information: type of attack (if known); and if there is a ransom demand. However, reporting information will vary case by case, and the most benefit will arise if reporters have access to an extensive list of relevant information, which is not mandatory. Reporters

	should also have ongoing access to update the information, and then can then opt to share further details as it becomes known/available. By detailing an extensive list of relevant reporting information without making it all mandatory there stands to be a greater overall benefit. By creating a small set of mandatory reporting requirements, the process initially generates a much greater view of affected parties and likely captures any need for greater intervention if broad campaigns are targeting Australian entities. If the reporting detail is too onerous, then the process runs risk of being seen as difficult, particularly while entities are navigating the workload involved with incident response and system restoration.
9. What additional mandatory information should be reported if a payment is made?	As above, no further mandatory information. However, the Government should have visibility if payments are made. It would be useful to have further optional questions which may help to provide broader understanding on what drivers occur in an individual case which can then assist in shaping better support and prevention strategies.
10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory	The approach should be for information sharing purpose. The reporting should align to the

burden on entities with less capacity to fulfil these obligations?	requirements about privacy, risk and for others to act upon. Suggestion to make the obligation mandatory for all businesses. However, maintain a tiered type of approach from simply a notification of an incident happening with very basic details for small businesses (name, business type, sector, contact information) through to more comprehensive obligations for large entities with resources and in-house skills to identify, report and share relevant information.
11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?	If the reporting limitation is set on turnover this may create a perverse incentive for criminals to target smaller entities with specific campaigns. Employee numbers, sector and business criticality may also be good measures to include a broader reporting base. Mandatory reporting also creates an opportunity for government to support businesses that have been the subject of an attack.
12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?	We suggest that a simple regime aligned with current practices would be most effective. The reporting requirements in SOCI provide a good starting point, and using these would serve to reduce the complexity that would be introduced by disparate requirements.
13. To what extent would the no-fault and no-liability principles provide more confidence for	Overall expect it would encourage higher levels of reporting. There will always be entities afraid to

entities reporting a ransomware or cyber extortion incident?	report due to risk of non-compliance (whether intentional or not), and the unknown legal terrain. There is also risk of potential legal and financial implications (i.e., civil suits, fines) in a domain which does not have precedents set. Also, this becomes difficult in a third-party situation if contractual issues are being debated, i.e., legal parties would not want anything reported.
14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?	Government can provide advice on how to best prepare and ensure they are aware of compliance obligations through relevant media campaigns and industry peak bodies. By providing an embargo period on compliance penalties and modelling positive examples through media.
15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?	We suggest an approach similar to that which has been taken in encouraging organisations to address their health and safety obligations. This approach has successfully encouraged greater understanding through accountability with senior executives and Boards. There needs to be tests of reasonableness when it comes to addressing non-compliance
16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?	The critical elements being shared need to be relevant and actionable for other entities. If the information relating to an incident are not easily applied in a broader context of another organisation, then sharing of information is not a worthwhile exercise apart from alerting to the existence of an

	issue. As for how frequently this information should be shared, the most effective sharing is done in a timely manner so ensuring the sharing process works in the most expeditious way to get information out to industry and government as soon as possible is best to attempt in mitigating further infections. At the strategic level it will be useful to share summaries of how many organisations in which sectors were impacted, and any campaigns evident from attacker behaviour. That could be 6 monthly.
Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator	
17. What should be included in the ‘prescribed cyber security purposes’ for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?	In the event of a cyber incident the assistance and sharing mechanism with ASD and the Cyber Coordinator needs to be directly relevant to the incident. To ensure this is the case, all requests for information regarding the incident should be contextualised in correlation to why the information is needed. Limitations should be applied to the affected system(s) and be able to be determined by the affected entity unless there are extenuating circumstances which may enact the additional SOCI step in powers.
18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?	Whilst in many cases it is hard to identify all elements of relevance relating to an incident, there needs to be a level of mutual cooperation to ascertain information relevancy or gaps. Initial

	documentation may include the need to share high level network or system architectures. The retention of any shared information should be destroyed post the incident, unless both parties agree there is relevance and benefit, and it meets the limitation of not being utilised for any regulatory or compliance means.
19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?	ASD and the Cyber Coordinator can provide anonymised case studies where the free sharing of information has resulted in benefits to the affected entity. Showing examples where the expedience of system restoration has occurred through this cooperation and sharing would go a long way to assist in developing public trust. Getting statements from affected parties to show how the process has been executed from their perspective would also assist in the broader public trust. There must be a truly secure portal for sharing of any such documents.
Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board	
20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?	A key to making this function successful is having a body of experts with key deliverables focused on learning, guidance and proposed tangible actions derived directly from an incident. The outcomes could relate to shaping policy, practice, government programs and industry risk management and controls. By developing a group with deep

	expertise, the benefits can be wide ranging and can be particularly beneficial for critical infrastructure entities. Limited use; high threshold; recognition will be very onerous for organisation being reviewed and will be an expensive exercise overall.
21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?	Ensure the key remit for the board is on post incident review and continuous improvement for process and risk management across government and industry.
22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?	Avoid board members holding positions in law enforcement or regulatory bodies, maintaining a demonstrably independent CIRB. Similarly, board members would need to demonstrate confidentiality, and the published findings from the CIRB must meet the objectives without implying fault. For example, consider a case in which an organisation lacked a vulnerability management program, and a 0-day in a VPN gateway allowed an attacker access. A report finding 'increase knowledge of threat actor use of 0-day' rather than 'implement a vulnerability management program' gives a specific action item for others to learn from, but also doesn't imply the organisation previously had no management of vulnerabilities.
23. What factors would make a cyber incident worth reviewing by a CIRB?	The first action of the CIRB must be to consult with the cybersecurity industry then develop and clearly

	publicise criteria (i.e., impact, risk, etc). It is already suggested in the document that existing thresholds could be used in order to provide a simpler, transparent framework. Note that "cost of conducting a review" is listed as a consideration. However, it is likely that incidents meeting the other conditions will be the costliest to investigate, therefore restricting investigations on cost alone should be very carefully managed.
24. Who should be a member of a CIRB? How should these members be appointed?	A governance system must be designed and publicised with clear purpose, scope, roles and responsibilities. Conflict of interest must be carefully managed, for example board members in for-profit organisations should not gain access to information they would not otherwise have. However, excluding certain industries could reduce available talent. A *pool of CIRB members* is therefore recommended to avoid COI on a per-incident basis. Similar to any other Board, firstly define the purpose, scope, roles and responsibilities, then establish the governance cadence to guide the selection.
25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?	There must be concerted effort to ensure no conflict of interest in decision making. A transparent interest register (or similar) is vital to ensure that the CIRB is both independent and seen to be independent.
26. How should the Government manage issues of personnel security and conflicts of interest?	As per other independent boards, noting the responses in Question 21 and 24 regarding a pool of

	members from different industries, to avoid COI on a per-incident basis.
27. Who should chair a CIRB?	CIRB should be operated as an independent board and elect its own chair.
28. Who should be responsible for initiating reviews to be undertaken by a CIRB?	As per the response to Question 23, the CIRB must consult, then develop and clearly publicise criteria. Some conditions are listed in the document, and the CIRB should also be open to accepting requests for review which fall outside the scope of those thresholds, providing sufficient conditions for review are met, considering the aim is to provide guidance and share lessons learnt with the public.
29. What powers should a CIRB be given to effectively perform its functions?	The CIRB should be conducted in a manner befitting the 'no fault' intent, by operating as a hearing committee not an investigative or audit body, using voluntary powers to request information. As noted, this approach will be key to gaining trust from the cybersecurity industry and achieving the intended outcome of sharing lessons learnt with the public.
30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?	The purpose of the limited use obligation for the ASD and Cyber Coordinator is to encourage industry engagement with government, to achieve the intended function of the CIRB. The CIRB itself will be comprised of representatives from various industries, and a separate limited use obligation must prevent misuse of incident review data. For

	example, a CIRB member must not use information gathered for commercial gain.
31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?	This is a difficult precedent to set. It is important to firstly build trust in this process and deliver outcomes. As noted in the response to question 13, without precedents in case law, the possibility of serious legal ramifications for technology and cyber faults is a risk to all businesses. Ideally, a grace period of at least 12 months with no enforcement or penalties on those who opt not to comply with CIRB is preferrable.
32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?	The CIRB members must have the upmost integrity for credibility. Understandably people, by design, are erroneous. The Membership would ideally comprise of people able to dedicate enough time to be thorough and effective.
33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?	This builds from the responses to questions 31 and 32; the CIRB must have the highest standard of information security. This CIRB will be highly scrutinised by public opinion if data theft or information leak occurs. Controls around information security should be well-established and maintained.

Part 2 – Amendments to the SOCI Act	
Measure 5: Protecting critical infrastructure – Data storage systems and business critical data	
34. How are you currently managing risks to your corporate networks and systems holding business critical data?	This differs across the sector, but mostly via education, segmentation, access controls, with oversight from Risk and Audit Board/Committee. Business critical data is open to interpretation within the legislation, and it would be great to support definitions with case studies. Generally, these are categorised as 'crown jewels' for any organisation and are prioritised in the risk-based approach to cybersecurity controls and focus.
35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?	If a Higher Education institution does not have any 'critical education assets', then this will not be relevant. If they do have any critical education assets, these would need to be linked (accessible via lateral movement) to the data storage systems in scope. This will limit the impact on Higher Education. Amendments should incorporate Privacy Act amendments (as noted in the strategy). Sector legislative burden and oversight is hefty, with much in review/pending, and correlation federally is imperative. Whilst a separate Cyber Bill (then Act) is great, it must not overstep on existing requirements (including state-based requirements).

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?	Any amendments introduce resource costs in an already stretched domain, and financial costs for asset identification, compliance activities, etc. However, these are a necessity if we hope for positive change to occur. Note, many Higher Education institutions do not have any critical education assets, and if they do, they may not be connected to the data storage/critical business data areas. Any new requirement is difficult in severely resource constrained environments. Higher Education organisations are not 'command and control' and harder to identify and then enforce.
Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers	
37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?	From current knowledge it is unlikely this would be relevant for a university. In the instance where there is a critical infrastructure asset it could help navigate some issues between industry partners and potential legal obstacles. When involving select research projects it would be helpful to then advise others that may be impacted as often the university would not know. This measure and commitment to assist in secondary consequences is great, as long as no further regulatory overheads are proposed as part of this process. Ideally, this would be an organic development throughout the incident following

	initial lodgement with ACSC/ASD, and after threat actors removed and services are restored. Given that post-incident is generally a time when response teams may be fatigued, it is a great opportunity for extra support. Navigating the post-incident legal and risks is something that is welcome; it is a complex landscape. Those impacted by a sector incident would include a large part of the population (i.e., students – current, former, future, research participants, staff – current, former, future, research bodies, etc). Given this large user base and the potential consequences, assistance in the most serious circumstances to help reduce impact on the population is welcomed.
38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?	Some State and Territory Governments offer incident support (i.e., bulk procurement opportunities), and the Federal Government should make use of these state-based resources where available.
39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?	The government must build trust. If not seen as an entity that will safeguard information with effective processes, there will be resistance in the uptake of these powers. Improved cybersecurity capability across Federal government entities is required.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions	
40. How can the current information sharing regime under the SOCI Act be improved?	The government has made positive developments in the form of the Trusted Information Sharing Network, Cyber Threat Intelligence Sharing platform, and local Information Exchanges. These initiatives are hugely valuable for industry, and we believe help industry and government to react to threats more quickly and decisively. Further consolidation and clarification of the information sharing ecosystem within government would be beneficial. An overview to provide clarity of responsible agency (such as a contact list of different Departments and functions, including State/Territory and Federal support) would be beneficial. The Cyber Security Response Coordination Unit/National Office of Cyber Security is an excellent initiative.
41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?	We support a harm-based threshold for information disclosure. The initial resource expenditure may be problematic for some but believe in the long term would provide greater visibility of information and would provide a feasible way to report information responsibility to executive.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers	
42. How would the proposed review and remedy power impact your approach to preventative risk?	The AHECS partners take their risk management obligations seriously and an additional review and remedy power would not change our approach to preventative risk. However, we see a consultative and collaborative approach to risk, such as that included in the TSSR/CIC process to be valuable.
Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act	
43. What security standards are most relevant for the development of an RMP?	n/a
44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?	n/a
45. How can outlining material risks help you adopt a more uniform approach to the notification obligation?	n/a
46. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?	n/a
47. How do your procurement and network change management processes align with the existing and proposed notification	n/a

arrangements? Can you suggest improvements to accommodate industry practice?	

Thank you for the opportunity to provide feedback on the Australian Cyber Security Strategy.

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

Nikki Peever – Director, Australian Higher Education Cybersecurity Service (AHECS)

Director, Cybersecurity, Council of Australasian University Directors of Information Technology (CAUDIT)

[redacted]

Karl Sellmann – Chair Executive Steering Committee, Australian Higher Education Cybersecurity Service (AHECS)

Chief Information Security Officer and Associate Director IDS Infrastructure, Flinders University

[redacted]

Mike Holm – Partner Representative, Australian Higher Education Cybersecurity Service (AHECS)

Senior Manager, AusCERT

Dave O'Loan – Partner Representative, Australian Higher Education Cybersecurity Service (AHECS)

Head of Cyber Relations, AARNet