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

Cybersecurity strategy discussion paper:
Australasian Higher Education Cybersecurity Service (AHECS) submission

Classification: Public

15 April 2023

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's 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 strategy. 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.

After consultation with AHECS Partners and Members, AHECS makes the following general recommendations regarding the 2023-2030 Australian Cyber Security Strategy Discussion Paper:

1. **Strategy timeline**

It is commendable that the Government is working to further develop the Australian Cybersecurity Strategy. However, we suggest that foreseeing the technology and security landscape over a seven-year period may be challenging. The cyber landscape is constantly evolving, and our defensive and offensive strategies need to be timely, agile, and responsive. It is important for the government to regularly review, validate and update our nation's cybersecurity strategy to ensure that it remains relevant, achieves the desired outcomes, and is responsive to changes in the cyber-threat and technology landscape.

Key recommendations

- We recommend that the panel focus on providing detailed guidance in the immediate future, e.g., 3 years, and provide general guidance in the outer years of the strategy period, noting the likelihood of expected technology and threat changes, and including details on how these will be managed/reviewed.
- Ensure that other mechanisms (outside of the Expert Advisory Board) are implemented to provide required inputs (e.g., technology R&D directions), which include mechanisms for action rather than solely advisory services.

2. **Focus on international relationships and strategic approach to positive cyber change**

To truly improve cybersecurity and reduce cybercrime, change is needed at a global level. International relationships and strategic networks are the only viable method for the prompt and significant uplift required against global cybersecurity challenges. The Government is best placed to encourage and impact these changes, which may be in the form of international law reforms (i.e., data protection regulations, cyber incident reporting requirements, international cooperation agreements, etc.) Cultural reforms at a

global level, such as promoting cybersecurity awareness and education among citizens, can help to mitigate risks and increase resilience against cyberattacks.

Additionally, it would be useful to look at international cyber strategies, such as the UK's active defence strategy, and the recently published US Cyber Strategy as much of the content can be appropriately reflected in an Australian context. For example, the US Strategy notes emphasis on technology providers and developers to do things ethically and correctly (i.e., follow the NIST Secure Software Development lifecycle, aim to meet the Software Bill of Materials (SBOM) initiative, and meet base level internet of things (IoT) security requirements). The strategy also notes the intent to uplift the weaker areas of the ecosystem, such as small-medium enterprises, local governments, charities/not-for-profits, and small vendors.

Key recommendations

- The Government should focus on the international landscape and improving the core issues leading to cybercrime and cybersecurity issues (i.e., law reforms, global awareness).
- Look to utilise comparable and established international cyber policies, and existing frameworks.

3. Education, research, and development (society-level cultural change)

We believe that a strong education and research sector is a key component of a resilient and agile economy, especially as it relates to cybersecurity. We encourage the panel to consider recommending increased investment in cybersecurity education, research, and development. This could include collaboration with universities and private sector partners to develop best practice, and innovative cyber solutions. Additionally, cybersecurity training should be available to individuals at all levels of society, including school students and small business owners.

Educating the public on cyber risks and teaching individuals the basics of how to protect themselves online can significantly reduce the overall risk landscape. Whilst it is important for businesses to incorporate cybersecurity controls in their environments, it is equally important for those using digital

services and technologies to have a basic understanding of cybersecurity, in the same way that all drivers gain an understanding of road rules before operating a vehicle.

Key recommendations

- Implement a comprehensive, sustainable cybersecurity education program.
- Develop a sustained, interactive awareness programme for all Australian citizens.
- Implement cultural responsibility across individuals, community bodies, government, organisations for digital selves, assets, and services.
- Increase investment in cybersecurity research and development.

4. Industry and peak body partnerships

Australian Government agencies have made significant leaps forward in the past several years in terms of their contribution to, and leadership of, Australia's cyber development. For example, the establishment of the Critical Infrastructure Centre, Australian Cyber Security Centre, ACSC Cyber Threat Intelligence Sharing platform and a wide range of other initiatives have meaningfully and significantly increased our economy's ability to respond to cyber threats. It would be great to continue maturing the current feeds and intel sources (i.e., CTIS), and look to local and international counterparts to provide curated intelligence and to draw actionable information from these capabilities (i.e., the New Zealand based Malware Free Networks (MFN) provided by the NCSC).

The Government should continue and further develop these capabilities and partnerships with industry. The private sector has significant expertise and resources and are equipped to collaborate with the Government to assist identify and respond to emerging threats and to develop innovative solutions. Additionally, the Government should encourage local Australian businesses to invest and uplift their own cybersecurity practices, leveraging private sector and peak body capabilities.

Partnerships can also foster a shared understanding of cyber risks and promote best practices across sectors. The Government should encourage collaboration and information sharing across sectors,

including critical infrastructure sectors, government, private industry, and academia. This would help to identify emerging threats and vulnerabilities and develop effective mitigation strategies.

Key recommendations

- Make use of the experience and technologies of Australian industry leaders and peak industry bodies.
- Incentivise businesses to invest in cybersecurity products and services.
- Support the development of local cybersecurity startups.
- Encourage information sharing and collaboration.
- Ensure there is a mechanism for continual feedback (360-degree cycle with appropriate bodies, i.e., Expert Advisory Board).

5. Responses to 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?	• We recommend that the panel consider leveraging industry and peak sector bodies to support execution of the strategy. • We believe that a focus on culture, incorporating leadership, policy, procedure, incentivisation, education, and awareness, are key to the success of this strategy. • We strongly support the development of Australian sovereign capabilities, especially through a pipeline of skills development and cultivating deep industry expertise. Universities and their capabilities can be a resource to help develop these capabilities. Strengthening existing industry initiatives and using government procurement strategically to support the development of a local industry can also be key tools.
2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?	• Incentives for businesses to undertake and achieve cybersecurity certification would help to develop capability in industry. • There should be an increased focus on supply chain security. This may involve implementing best practice supply chain risk management guidelines or incentivise businesses for achieving cybersecurity

	certification which specifies supply chain controls (i.e., ISO27001). • Further privacy reforms (including many of those recommended in the 2023 Privacy Act Review Report) will help to encourage protection of personally identifiable information and sensitive data. • When legislation (or proposed legislation) incorporates fines for breach, those fines should be proportional to the financial size of the organisation.
2a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?	• Guidance, education, and support • Board and Director duty reform (see response to 2.c. below) • Minimum obligations (e.g., minimum road safety knowledge when attaining a driver's licence – no different). Make it personal and phase in the requirements.
2b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?	• No further reform suggested, but more support for critical infrastructure sectors, and between sectors collaboration. • We support the current risk-based approach. • Reviewing the current separate federal and state-based incident response and reporting requirements, to refine and set a collective

	national strategy, would better support and make better use of resources for those impacted by cyber incidents. Most critical infrastructure rely on other critical infrastructure, so these need to be more than sector based with support for inter-sector collaboration.
2c. Should the obligations of company directors specifically address cyber security risks and consequences?	• Yes. We suggest that clarity around director duties would be helpful both for directors themselves and to ensure appropriate company governance. In terms of governance arrangements, we do not advocate introducing new arrangements that treat cyber risks separately from general corporate risks as we believe that treatment of these risks needs to be taken together to ensure that they are governed appropriately, and together.
2d. Should Australia consider a Cyber Security Act, and what should this include?	• We don't believe this is specifically necessary because of the strong likelihood of overlap with existing legislation/regulation, for example, the Privacy Act, TSSR and SoCI. • Should consider (and improve) how state-based legislation interconnects.
2e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are	• There are opportunities to unify state and federal level legislative and regulatory

there opportunities to streamline existing regulatory frameworks?	requirements, for example as they relate to privacy. We note the current Privacy Act Review Report and are encouraged by the recommendations that seek to bring Australian law into line with international best practice, e.g., GDPR. • Significant opportunity to streamline regulatory frameworks and commitments, but also an opportunity to change this to be a positive position for many businesses in a competitive, global market.
2f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?	• In principle, we support a prohibition on the payment of ransom demands. However, we suggest that the implementation of such a prohibition needs to be carefully considered to take account of, for example, situations where life may be at stake if a ransom is not paid.
2fi. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?	• If Australia is known as a country that does not pay ransom, then will likely be less targeted/less focus for criminal groups. • Companies would know that this option / safety net isn't available, so would potentially take a different view towards their digital safety (similar to many businesses with their physical security).

2g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?	• Yes. Clarity on this would help organisations to prepare for cybercrime while serving to discourage cyber criminals as per our response to 2.f.i. above.
3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?	• Shared threat intelligence (industry included). Improvements to the CTIS initiative, support for shared development / understanding and defences. Per recommendation 2, utilising local and international counterparts to provide curated intelligence and to draw actionable information from these capabilities (i.e., the New Zealand based Malware Free Networks (MFN) provided by the NCSC).
4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?	• Connect into established international bilateral and multinational partnerships for other areas and support / foster the development of cybersecurity included within them.
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?	• Australia should contribute to international standard setting, but, to date, we have acted independently. There are international regulations such as GPDR that could be used as a de facto international standard that many Australian businesses must already comply with.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?	• The Government should be realistic with industry (i.e., not hold themselves higher than industry) and collaborative, as the Government are also prime targets for threat actors (both e-crime and nation state based). Is the Government meeting essential 8 internally, and therefore, how does government serve as a model? Sufficient resources and direct cultural influence to building in cybersecurity practice should be mandated and evident.
7. What can government do to improve information sharing with industry on cyber threats?	• We appreciate that, in order to maintain participants' trust, information sharing processes need to take account of confidentiality expectations. the current regular information sharing with operators of critical infrastructure is an excellent start. The current approach of desensitising information prior to sharing more broadly can make it challenging to act upon that information.
8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC	• This is difficult as a blanket explicit obligation can be a hindrance in the timeliness to response. The risk to a business of a cyber incident is similar to other business risks – would you have them reported as well? A risk-based approach may be a better consideration.

without the concern that this will be shared with regulators?	• Any obligation would need to be considerate of other laws and an individual's and businesses rights as well. • The current reporting portal would benefit from improvement to ensure fitness for purpose. Ideally, a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators would be beneficial.
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?	• ABS, benchmarking, and exemplars would dispel animosity and help change culture. It would not address individual, community-based awareness and responsibility challenges.
10. What best practice models are available for automated threat-blocking at scale?	• This is a space that is likely to evolve significantly in the upcoming years, and ideally solutions utilising cyber resilience (rather than cybersecurity) and machine speed threat identification and adaptive controls response (i.e., NIST.SP.800-16-v2 as a framework). Currently, there are examples of manual threat blocking at scale based upon intelligence gathering and sharing in specific sectors (happy to discuss these if required). We suggest that education and awareness coupled with technology provide

	a more complete solution in current times, although this is likely to evolve to primarily technology based within the next five years.
11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?	• Yes. We believe that there is a key role for Australia's universities to play in ensuring that our economy has a strong pipeline of skilled workers in this area. Research and development capabilities further strengthen our ability to respond to changes in the landscape and should be considered when addressing skills.
12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?	• Partner with higher education and research to advance relevant research. Bursaries for higher education research relevant to cybersecurity (and other national interests). • Ensure cybersecurity is part of K-12 standard education program which has the potential, if addressed correctly, to address diversity within STEM showing cyber as a career for all. Ensuring we have a diverse cyber workforce delivers a number of significant benefits including increasing the number of potential cyber workers just by having diversity.
13. How should the government respond to major cyber incidents (beyond existing law	• The Government currently hold step-in powers for critical infrastructure providers. The Government could develop a reporting

enforcement and operational responses) to protect Australians?	process for Australians affected by compromises, to provide a consistent and integrated approach (i.e., incorporate existing federal and state systems).
13a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?	• Yes, per question 8. The current reporting tool is a basic static style form that requires maturity improvement to provide access to continually update as information is found pertaining to incidents, as well as reporting back to the reporter for record keeping.
14. What would an effective post-incident review and consequence management model with industry involve?	• This should be handled by existing industry leaders; no need for Government to reinvent existing mechanisms (that currently work).
15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?	• Education and awareness play a key role in addressing this at a population level. Government resources and incentives can help to ensure that cybersecurity is part of K-12 education program. Incentivise small businesses to undertake accreditation and cyber training. Partner with existing industry providers regarding identity protection and post-incident personal support services.
15a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?	• Incentives for businesses (small, medium, and large) to gain accreditation and undertake relevant training.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?	• Per earlier responses, investment in local capability, including startups, to address the challenges, and aligning the cyber education with industry to connect the brightest current and emerging minds with industry to ensure local retention, while also providing resourcing for industry to succeed.
17. How should we approach future proofing for cyber security technologies out to 2030?	• A long-term approach to future proofing technologies is unrealistic, beyond continuous review and investment. This is a human issue as much as a technology issue. Technologies will continue to change and adjust, mechanisms, principles and culture will best place society's ability to proactively challenge emerging technologies and capabilities. It is important that proactive approaches, understanding current capabilities and ensuring that adequate support is in play to adjust and evolve as is required.
18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?	• Yes, government procurement can be used to support the development of a local cybersecurity ecosystem and particularly can help develop smaller, more innovative players in that ecosystem. We believe that with a strong cyber-security research capability, Australian industry can be a leading innovator in this area.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?	• In-line with our opening comments, we support the Australian Government providing a long-term strategic vision for our cyber capabilities and industries. However, we suggest a focus on the immediate-term challenges that our economy faces in this space. The strategy should provide for emerging technologies and subsequently threats to be continuously assessed, proactively monitored, and ensure the implementation of agile processes to enable industry and government agencies to respond quickly to changes. Supporting bodies (supply chain, research bodies and community / peak bodies) play a significant role in this capability chain.
20. How should government measure its impact in uplifting national cyber resilience?	• Utilise the ABS towards gaining KPI measures within the community. KPIs should align to principles outlined in the cybersecurity strategy.
21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?	• There is a delicate balance between keeping citizens informed and not giving away secrets to criminals. Government strategy should remain high level, with CI or sector based ongoing evaluation.

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 the recommendations or comments, please contact:

Greg Sawyer – Chief Executive Officer

Council of Australasian University Directors of Information Technology (CAUDIT)

[redacted]

Nikki Peever – Director, Cybersecurity

Council of Australasian University Directors of Information Technology (CAUDIT)

[redacted]

Karl Sellmann – Chair, Executive Steering Committee

Australian Higher Education Cybersecurity Service (AHECS)

[redacted]