CAUDIT
Council of Australasian University Directors of Information Technology

Australia's 2020 Cyber Security Strategy

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 call for views on Australia's 2020 Cyber Security Strategy.

CAUDIT is the peak member association supporting the use of information technology in the higher education and research sector in Australasia. CAUDIT is a registered Not-For-Profit Association with 62 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.

The current CAUDIT Executive committee, providing the governance of CAUDIT, is:

Position	Name	Role	Institutions
President	Gina White	Director, Technology Services	Southern Cross University
Vice-President	Kerrie Campbell	Chief Information Officer	Flinders University
Treasurer	Scott Sorley	Executive Director (ICT Services)	University of Southern Queensland
Secretary/ Public Officer	Kerry Holling	Chief Information and Digital Officer	Western Sydney University
Past-President	Niranjan Prabhu	Chief Information Officer & Director	Australian Catholic University
Ordinary Member	Warwick Calkin	Chief Digital and Information Officer	The University of Western Australia
Other - NZ Rep	Eion Hall	Chief Information Officer	University of Waikato

CAUDIT members prioritised Cybersecurity in 2018 as the number one initiative for CAUDIT to address for the Higher Education sector. CAUDIT, partnering with Australia's Academic and Research Network (AARNet) and AusCERT, is developing the Australasian Higher Education Cybersecurity Service (AHECS). Research and Education Advanced Network New Zealand (REANNZ) has since joined the partnership to ensure this is a truly Australasian service for the sector.

AHECS will support 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 will be achieved by AHECS coordinating 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.

By having this coordinated approach, built on an established framework (NIST) and backed by delivery, we can collectively more easily ensure 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 selected partners including FifthDomain, 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, as well as the general community, in ensuring the development of our nation's next Cyber Security Strategy and commitment to protecting Australians from cyber threats.

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 call for views on Australia's 2020 Cyber Security Strategy and correlate the member feedback. The working group membership is:

Position	Name	Title	Institution
Chair	Anne Kealley	Chief Executive Officer	CAUDIT
Member	Greg Sawyer	Strategic Initiative Development Manager	CAUDIT
Member	Karl Sellmann	Deputy Director: ISTS	University of South Australia
Member	Mark Brodsky	Associate Director, IT Strategy and Program Delivery	Australian Catholic University
Member	Tim Lane	A/Senior Manager, Risk and Compliance	Griffith University
Member	Geoff Still	Project Manager, Cyber and Information Security	Southern Cross University
Member	David Hird	Security, Standards and Compliance	La Trobe University
Member	Joshua Quek	Cybersecurity Architect	The University of Western Australia
Member	Damian Walker	Chief Information Security Officer	CSIRO

Thank you for the opportunity to respond to call for views on Australia's 2020 Cyber Security Strategy. CAUDIT's response to the call for views identified the following key recommendations.

1. **Strength in unity, scale and efficiency.** 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.

   Recommendation: The Government address the current allocation of responsibilities to strengthen support and foster connections between government, sectors and industry groups active in this space.

2. **Education.** Apply a risk-based approach and address the soft targets. The soft targets include the older demographics that may be less cyber literate and for who education has the potential to raise their ability to correctly respond to common attack vectors. Education can be achieved through building capability, community education and providing certified qualifications for higher levels of cybersecurity development.

   Recommendation: The Government scale efforts to embed cyber security in education and training to produce a highly-skilled cybersecurity workforce.

3. **Awareness.** An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (SunSmart, quit smoking and tourism), cybersecurity needs a voice so that the community is aware and informed. Increase proactive focus on cybersecurity as another risk - on equal footing with other national, organisational and individual risk. The development and promotion of guidelines, including promoting awareness, will underpin the government response to the threat landscape.

   Recommendation: The Government commits to, funds and effectively leads the national conversation, raising awareness within the general public and SMEs on an ongoing basis.

4. **Communication.** Clear and visible communication of expectations, existing law and repercussions of infringement. One channel to the community and a consistent message across government functions to avoid mixed, ineffective and inconsistent communication.

   Recommendation: The Government review the communication strategy across government functions and provide guidelines to ensure a clear, consistent message to the community.

5. **Transparency**. Improving transparency and clarity around the different agencies and activities involved in cybersecurity will assist in building community trust and increasing the effectiveness of the cybersecurity communication.

   Recommendation: The Government re-examines guidelines and agency interactions to improve transparency, communication and clarity.

6. **Standardisation**. Government provision of standards and guidelines E.g. re compliance requirements within verticals. A strong preference for guidelines over and above restrictive legislation as a means of improving the maturity ecosystem. Some verticals, e.g. defence, may have stronger guidelines than others, e.g. education. Cybersecurity is not a 'one size fits all' scenario.

The government could provide a marketplace for services. Qualification around suppliers e.g. re the energy sector. The 2020 Cyber Strategy should provide a common language for cybersecurity, allowing a baseline for cybersecurity risk management and allowing cybersecurity to be considered in the same way as other risk domains e.g. Finance, Work Health and Safety and Human Resources.

Recommendation: The Government provides standards and guidelines, ensuring review of compliance requirements within verticals.

7. **Cyber emblem**. An emblem to recognise goods and services that establish a base level of cyber protection. This will support building awareness, developing a culture of cybersecurity within the supply chain and provide Australian service providers with an opportunity to differentiate their service offering.

Recommendation: The Government implements a readily recognisable emblem for goods and services that meet a base level of cyber protection.

8. **Ecosystem.** An ecosystem of cybersecurity aligned and underpinning each other, focused on the collective improvement of Australia's cybersecurity landscape. Engagement, building and supporting relationships to improve engagement within the ecosystem.

Recommendation: The Government 2020 Cyber Strategy underpins the cybersecurity ecosystem as a whole rather than piecemeal approaches to individual elements.

9. **Incentivise cyber**. Cyber needs investment and through prudent Government expenditure 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 the regional communities, and funding to agencies, like AustCyber, is proportional to the challenge and eligibility scope broadened to support developing the ecosystem to underpin the 2020 Cybersecurity strategy.

Recommendation: The Government incentivises investment in cyber across all sectors and verticals to address the ever evolving challenges and broaden the ecosystem underpinning cyber security.

10. **IoT.** There are emerging technologies with potential broad impact, like the Internet of Things (IoT), where the industry is maturing. Australia could be a world leader in IoT cybersecurity as this is both a potential opportunity and risk. Integrate research into Universities and Centres of Excellence, and invest in real-world application of IoT, potentially government buildings, to demonstrate the commitment, capability and outcomes of the solutions.

Recommendation: The Government provide guidelines, and lead by example, to ensure a robust technology and research investment ecosystem which places Australia as a world leader in all facets of IoT.

CAUDIT, with input from its members, provides the following responses to the 26 questions laid out in the Call for Views document:

Q No.	Question	CAUDIT Response
1	**What is your view of the cyber threat environment? What threats should Government be focusing on?**	The cyber threat environment consists of a variety of new and rapidly evolving threats to government, industry, academic and individuals. These range from nation state intelligence type actors/threat to relatively unsophisticated threat actors with access to publicly available tools and information that can be used to compromise individual and organisational interests. Security is 'a team activity' that the government needs to lead. Artificial intelligence and IoT have potential to be a boon to both threat actors and those seeking to limit their impact. Government should focus on providing fit for purpose guidelines and practical advice for each sector of the economy. Legislate as a tool should only be completed through exhaustive, consultative engagement with in-built protection to ensure the legislation is measured against the outcomes. Legislation administered poorly can affect adversely innovation. **It is recommended that the government focus on threats to 'national' infrastructure (noting that some of this is managed by states/territories or non-government organisations) and the well-being of its citizens.** Uplifting the data governance capability and security incident response within this context are key outcomes. The Government is now considering that 'research and research data' is of national interest through the University Foreign Interference Taskforce work. Research and research data could be formalised as national infrastructure, recognised as such by the Government. In the same way Hospitals are recommended to be considered as 'national infrastructure' worthy of support with recent examples of the risk to the community from effective cyber-attacks. The increasing prevalence of IoT, in both the research and hospital environments increases the risk profile in these environments.
2	**Do you agree with our understanding of who is responsible for managing cyber risks in the economy?**	Yes, we agree, the ecosystem includes governments, academia, industry and the community. However, more attention needs to be paid to the interactions between each of these groups to remove silos. By working together, and leveraging the strengths and attributes of each group, the nation's cyber resilience will mature.Consideration for end-users needs to be addressed, reflecting end-users will not understand the complexities and landscape to be able to adequately respond to the increasing cyber threats. Mechanisms are required to provide for end-user safety including awareness and emblems to identify cyber secure goods and services.It is suggested that industry groups could play a key role in the ecosystem. Clarity around the groups which represent each sector needs to be addressed to ensure accurate representation. The industry groups would provide a custodian role for the respective industry, assisting in developing guidelines and/or shared service in partner with relevant Government agencies.

3	**Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**	The current allocation of responsibilities requires improvement to reflect the network of connections, interaction between sectors and groups. The capability and capacity of government agencies requires to adapt to the changing threat landscape and provide proactive approaches to address the disparity between smaller organisations and SMEs, and the threat actors. There will always remain strength in unity, scale and efficiency. JCSC is well placed to have an expanded role, proactively engaging with the various groups within their region and being the local resource as an initial point of contact for cybersecurity expertise.
4	**What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**	The role of Government in addressing the threat landscape is significant. Cyber threat intelligence consolidation and awareness requires working with other Five Eyes countries to gather cyber threat intel, providing advice and automating cyber threat intelligence feeds to institutions and business and leading the cyber threat intelligence strategy domestically. An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (drink driving, sun safety, healthy heart), cybersecurity needs a voice so that the community is aware and informed. Increase proactive focus on cybersecurity as another risk - on equal footing with other national, organisational and individual risk. The development and promotion of guidelines, including promoting awareness, will underpin the government response to the threat landscape. The Government leads engagement and advice with diplomatic discussions to bring influence to address the threats, that institutions and businesses have no capacity to affect. These channels can reduce the likelihood of attacks from nation states, or at least raise the awareness that Australia is proactive and will not be an easy target. Detection and response to threat actors that the other groups cannot, in particular nation-state, requires Government to address and bring resources to bear to support affected institutions and businesses.
5	**How can Government maintain trust from the Australian community when using its cyber security capabilities?**	To maintain and build trust, the Government needs to be more transparent. Raising awareness of cybersecurity and providing leadership, will support transparency and increase trust within the community. Improving consistency between jurisdictions - layers of government - international, national, state, local. Cybersecurity is a national issue and the Government needs to ensure that a consistent, effective national approach is adopted backed by raising awareness within the community.
6	**What customer protections should apply to the security of cyber goods and services?**	Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. As there is already legislation around privacy, interactions with privacy, data governance and ownership guidelines require strong alignment between the proposal from a security perspective.

7	**What role can Government and industry play in supporting the cyber security of consumers?**	Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem.An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (drink driving, sun safety, healthy heart), cybersecurity needs a voice so that the community is aware and informed.Improve transparency of law and repercussions of infringement, education of victims including reporting and support available. A demonstrated public no blame point-of-view for victims of cyber-attacks will encourage reporting.After a breach notification - publication of lessons learnt where possible. Backing the no blame point-of-view, the lessons learnt will provide opportunities to share within recrimination and allow organisations, particularly those in the same vertical sector, to act on the lessons learnt and proactively address the risks within their organisations.
8	**How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**	Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. After a breach notification - publication of lessons learnt where possible. Backing the no blame point-of-view, the lessons learnt will provide opportunities to share without recrimination and allow organisations, particularly those in the same vertical sector, to act on the lessons learnt and proactively address the risks within their organisations. Government and industry can raise the effectiveness through standardisation and compliance of digital offerings. Tying back onto the emblem for goods and services that establishes a base level of cyber protection, standardisation and compliance will address the base level and provide consumer awareness of the capability of the goods and services in relation to cyber.

9	**Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**	Government will need to maintain or control all functions that relate to nation-state actors. The risk of the private sector being influenced by profit over cybersecurity are too great in an immature market. Critical infrastructure, especially of nation state importance, requires a very close alignment to the Government, noting that services including hospitals have already been privatised, and successfully breached.Where private sector devolvement is considered, a risk-based approach reviewing environment and threat is required to ensure cybersecurity accountability is addressed in the privatisation. An alternative to privatisation is an independent Government agency to provide the function and ensure increasing cybersecurity posture and maturity remain the key outcomes.Improve clarity on the expectations of cyber insurance industry through provision of standards and guidelines detailing in both in legal and plain English what is covered, terms, timing, service levels and outcomes from enacting cyber insurance.The effects of privatisation can provide economic efficiency, increased competition and reduce political interference. In privatising cybersecurity, consideration would need to address the ability of the private sector to maintain and improve the cyber posture of that function. Privatisation may affect regional services as the market is not sufficient to potential provide cost effective delivery of the function and privatisation has resulted in increased costs were the underlying principle of the private sector is profit, which may be counterintuitive to increasing cyber maturity and safety.
10	**Is the regulatory environment for cyber security appropriate? Why or why not?**	The regulatory environment for cybersecurity is not appropriate at present, predominantly built on dated and incomplete legislation, is not reflective of the changing threat landscape and rapid rise in changing cyber threats with variation across regions, states, and industry sector verticals. There is and will remain an ongoing competitive tension and connection between cybersecurity and privacy. In further regulation is deemed required, it needs to be mindful that other areas are implementing regulation, for example the DISP framework for compliance and accreditation. Legislation, as an outcome, needs to be consistent across jurisdictions, work cohesively together and be easy to understand. The University Foreign Interference Taskforce preference toward guidelines and policy over legislation is a positive approach.
11	**What specific market incentives or regulatory changes should Government consider?**	In relation to incentives, implementing cybersecurity steps and improving maturity will come at a cost. The cost burden can often be substantial, especially for smaller institutions and SMEs. Incentives for early adopters and achieving levels of certification could be provided through tax incentives. These could provide tax recognition through investment addressing cybersecurity challenges and encouraging innovation in cybersecurity for small businesses and universities. Increase funding to agencies such as AustCyber and support to industry groups will be required, at scale, to incentivise the market. Recommendation: Consider broadening the scope of eligibility, increasing the funding, support post start-up phase and commercialisation of innovation. Incentives could be made available to organisations and business who broaden support and scope of services made available to small organisations and SMEs. Regulatory changes are only recommended in ensuring that the existing regulatory domain is coherent and consistent across the Government landscape.

12	**What needs to be done so that cyber security is 'built in' to digital goods and services?**	Cybersecurity is best addressed as a continuum, and by building a capable ecosystem and nation. Shifting the culture in a full cybersecurity ecosystem, to one which is focused on supporting each other and on collective improvement of Australia's cybersecurity landscape, rather than one that is driven by legislation. Initiatives and incentives may create more market demand for new and existing services with cyber security built in by design. Awareness creating value in cybersecurity certification driving built-in cybersecurity to achieve certification. Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. The emblem needs to have key services baked into the offerings including appropriate password policy, two factor authentication, secure protocols and where applicable, address the IoT risk. An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (drink driving, sun safety, healthy heart), cybersecurity needs a voice so that the community is aware and informed.
13	**How could we approach instilling better trust in ICT supply chains?**	Creating a market opportunity for Australian through incentivising and encouraging business to participate in supply, not just consume from external supply chains. Cybersecurity is best addressed as a continuum, and by building a capable ecosystem and nation. Set standards for all supply chains ensuring domestic markets are competing under the same environment as imports, provide transparency and education to suppliers to ensure they can adapt to the requirements of being a cyber friendly supplier. Government contracts need to likewise incentivise the domestic market, open the government contracts to all sectors and SMEs to scale the marketplace and invest in valued, high quality supply chain capability with contracts over a long period to minimise the barriers to entry into the supply chain. Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (drink driving, sun safety, healthy heart), cybersecurity needs a voice so that the community is aware and informed.

14	**How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**	According to the latest census data, Australians are already upskilling like never before, and more than half the population now holds a post school qualification. The uptake of Information Technology related studies has also gone up by about 25 per cent in the past five years. The conditions are right for the government to scale efforts to embed cyber security in education and training to produce a highly skilled cybersecurity workforce. The focus should be on lifelong learning, commencing through school, embedded in graduate qualifications and incentivised through ongoing professional development ensuring future generations have digital and cyber literacy in their DNA. Increase the “human capital flight pull factors". The cybersecurity training ecosystem provides a variety of skills and training options, focused where this is best provided. University (UG, PG), TAFEs, short courses, life-long learning, Internships and Scholarships. Expand idea of Cybersecurity Centres of Excellence ecosystem. Attract from an early age, like the focus we have had on STEM in schools, recognising that cybersecurity is not just about STEM and focus on the positive of a career in cybersecurity. The target audience is domestic students. The time is now. Similar to teaching and medicine in remote areas, explore opportunities to ensure the skill base has an opportunity to stay in Australia and support regional communities, rather than chase higher remuneration overseas. Opportunities to have programs to provide employment on graduation within Government or regional areas where there is a financial incentive that is attractive against the international marketplace, like reduced tax, funded remote living costs and reducing HECS debt for a period served. Government provides skeleton/framework that the ecosystem is built around. There is an opportunity to target the low hanging fruit, the older demographics that may be less cyber literate and who education has the potential to raise their ability to correctly respond to common attack vectors. Supporting parents through training on the digital footprint and security hygiene. Australia is ideally placed to be a point of excellence in cybersecurity.

15	**Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?**	The cyber insurance market, especially domestically, is a relatively immature market at present. As understanding increases costs may increase or more niche products might be developed leading to more confusion. Improved clarity on the expectations of cyber insurance industry through provision of standards and guidelines detailing in both in legal and plain English what is covered, terms, timing, service levels and outcomes from enacting cyber insurance. The lack of clarity and understanding in regards to cyber insurance coverage may also lead to organisations having adequate essential safeguards and practices, falsely believing that cyber insurance provides protections. Lack of transparency surrounding cyber insurance in terms of how likely it is to pay on claims, how accurate all information provided needs to be and to what extent it is assessed on a claim and the statistics on cyber insurance across the industry would be helpful. Minimum viable policy could help, and standardisation of what policies cover would provide a base line.The introduction of 'back door' legislation may impact insurance coverage and affordability. There remains an ongoing discussion on ensuring greater clarity on security over privacy. The security of the nation and any security response needs to be proportionate to the threat but with a careful balance between the interests and values of the community. Consultation between the community, intelligence and law enforcement agencies, and the government more broadly remains as active in the future as it is today.
16	**How can high-volume, low-sophistication malicious activity targeting Australia be reduced?**	Encourage targeted activity by telecommunication sector, supported by the Government and intelligence agencies, to block malicious activity 'at the border' and on their networks. There would need to be controls and expedient processes to ensure the blocks are proportionate to the threat to ensure accountability and a review processes for unforeseen untoward outcomes associated with the blocks. The sector would require guidelines to provide the minimum standard. This protection would be baked into service offerings and provide protection raising Australia's overall posture, discouraging attacks on Australia as an easy or soft target. The blocks also potentially will remove the noise from systems closer to the consumer and community, ensuring these systems are more tuned to threats targeting these systems than having scale to dispose of huge volumes of unsophisticated attacks.

17	**What changes can Government make to create a hostile environment for malicious cyber actors?**	Through the creation of a cybersecurity ecosystem that is coordinated and provides a concerted effort nationally to continually raise the cybersecurity posture, leverage this underpinning capability to ensure the risk vs reward place Australia in the high cost, lower value category. The ecosystem will have transparency, sharing of good practice and within sectors, industry groups leading the sector providing base capability, services and templates that underpin strengthening the sector. We need to support building of offensive capabilities, potentially within government, to ensure threat actors understand Australia is a hostile and difficult environment for malicious actions. The Government is the 'Border Patrol' for cybersecurity.Continuing to raise awareness by promoting and encouraging media reporting on successful prosecutions, showing visibility of actions and apply a risk based approach. Address the soft targets in the community, our aging population who do not have the digital literacy that other generations possess. Provide community education and value addressing the soft targets. Every improvement helps to build and strengthen the hostile environment for malicious cyber actors. There is an opportunity to develop curriculum from Kindergarten through to HE so that citizens entering into any industry have basic cyber skills, as well as having the tools to address the ongoing day to day threat landscape that they will be exposed to. This would be integrated into the awareness campaign, providing to the multifaceted nature of the campaign.
18	**How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?**	No response.
19	**What private networks should be considered critical systems that need stronger cyber defences?**	No response.

20	**What funding models should Government explore for any additional protections provided to the community?**	Increasing amounts of funding are required to be made available to address what the Government document as the rising volume and sophistication to cybersecurity attacks. All funding should be aligned to risk, complexity and scale. A framework, like the NIST framework, can be utilised to assist in reviewing the risk and communicating the outcomes. An effective awareness campaign is required to ensure cybersecurity is front of mind for consumers. Lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness, not just once per year in Cyber Awareness week. Similar to other national campaigns (drink driving, sun safety, healthy heart), cybersecurity needs a voice so that the community is aware and informed. Education is a key component of the cybersecurity ecosystem. The uptake of Information Technology related studies has also gone up by about 25 per cent in the past five years. The conditions are right for the government to ramp up efforts to embed cyber security in education and training to produce a highly skilled cyber security workforce. The focus should be on lifelong learning, commencing through school, embedded in graduate qualifications and incentivised through ongoing professional development ensuring future generations have digital and cyber literacy in their DNA. Increase the “human capital flight pull factors". Similar to teaching and medicine in remote areas, explore opportunities to ensure the skill base has an opportunity to stay in Australia and support regional communities, rather than chase higher remuneration overseas. Opportunities to have programs to provide employment on graduation within Government or regional areas where there is a financial incentive that is attractive against the international marketplace, like reduced tax, funded remote living costs and reducing HECS debt for a period served. Government provides skeleton/framework that the ecosystem is built around. Increase funding for the education and awareness to agencies such as AustCyber and IDCare, and support to industry groups will be required, at scale, to incentivise the market. Consider broadening the scope of eligibility, increasing the funding, support post start-up phase and commercialisation of innovation. Ensure that the feedback mechanisms are also appropriate and encourage reporting and feedback providing a full feedback mechanism.
21	**What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?**	Awareness of the work that the government completes on behalf of the nation are not understood outside the technical, intelligence and government communities. The community as a whole is largely unaware. The option to provide an ‘opt out’ advice list that provides a clear understanding of the benefits of the communication to the recipient, to ensure they are engaged in the content. Transparency, communication and clarity will assist the Government with information sharing. Profile services that are available including AusCERT and the opportunity to partner with JCSC. Incentives could be provided to utilise and join domestic service providers, like AusCERT, to grow domestic capability, retain resources and increase maturity.

22	**To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?**	Strongly agree that the lack of cyber awareness results in poor consumer choices, but equally there is limited information available in the supply chain to make an informed decision. Consumers, generally, do not attribute a value to this. Scammers are becoming more sophisticated and the lack of awareness by the consumer further exacerbates the challenge to drive informed decisions. Implement a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. Within the workforce, there is an opportunity to provide training for all employees with certification, that could be in the form of a micro credential, that will recognise cyber training. This could be a government led initiative that provides benefits to all through raising awareness and also providing employees with transferable personal skills. This would also tie back into education and growing the domestic training market.
23	**How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?**	An informed population will demand improved services. Increased demand provides an opportunity to build Australian services with high quality, domestic focused, local supported solutions being a key differentiator. This could be along the lines of the Aussie lamb campaign, and ties back to the branding through an emblem for services and organisations that establishes a base level of cyber protection Additional value that will be derived is the potential to provide an export opportunity, transferability through improved integration between sectors, the intangible benefits around a maturing cyber aware population and the trust to buy online knowing, through the cyber emblem, the services are cyber smart. The Government should take a leadership approach on awareness. Media is currently leading and this will always be a fear based message. Government needs to provide a positive message to the individuals who feel the least empowered of all groups. Awareness campaigns have not in the cybersecurity space been effective in garnering brand recognition and retention within the Australian community, and therefore have yet to affect consumers driving the need for secure products.
24	**What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?**	There are a number of examples of successful campaigns that have moved and inspired consumers to change their behaviour and/or adopt something new.The campaign should have a simple enough message yet to a large degree persuade the targeted audience understand the importance of cyber security and become more cyber aware. We encourage experts in this space to contribute to the national conversation on this. The campaign needs to be positive, engaging, at the right level, refreshed regularly, ongoing and not rely on shock value to land the cyber message. This could be along the lines of the Aussie lamb campaign, and ties back to the branding through an emblem for services and organisations that establishes a base level of cyber protection. Other successful public service campaigns include SunSmart, quit smoking and tourism. The outcome must be awareness and understanding in the market, applying pressure to the supply chain from the informed community to ensure cyber security is a valued commodity.

25	**Would you like to see cyber security features prioritised in products and services?**	A consideration of standards aligned to capabilities, risk and feature would be beneficial. Simplified signs for easy and transparent understanding across government, industry, academia and individuals would be required. Start with implementing a readily recognisable emblem for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that adopt the emblem. Additional focus on emerging technologies with potential broad impact, like IoT, where the industry is maturing and Australia could be a world leader in IoT cybersecurity. Integrate research into Universities and Centres of Excellence, and invest in real world application, potentially government buildings, to demonstrate the commitment, capability and outcomes of the solutions.
26	**Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?**	To help inform the strategy, analysis should be undertaken to determine what has and hasn't been successful to date. A clear definition of 'success' needs to be included in the 2020 Strategy. Consider interrelations with other policy areas. What other considerations have been made to incorporate existing controls from other areas e.g. telecommunications and should there be elements added within other policy e.g. Fair Work Act, Public Sector Management Act? Government engagement with 'world' suppliers for conversation on IoT or commodity type products; development and promotion of safety guidelines - CHOICE.

Thank you for the opportunity to provide feedback to the Review.

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]