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

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Australasian Higher Education Cybersecurity Service (AHECS) submission

Classification: Public

18 August 2025

The Australian Higher Education Cybersecurity Service (AHECS) welcomes the opportunity to contribute to the consultation process to develop Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. As the peak national coordinating body supporting CIOs and CISOs across the Australasian higher education and research sector, we provide sector-wide threat intelligence, capability uplift, and collaborative security programs. The higher education sector is both an operator of critical infrastructure and a custodian of sensitive intellectual property, personal data, and cutting-edge research with direct implications for national security and productivity.

Our submission addresses the consultation areas most relevant to higher education, focusing on cyber messaging, critical infrastructure obligations, regulatory impacts, workforce and research, technology adoption, and ransomware/insurance challenges.

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. We encourage each partner or member institution to provide their own individual submission, as appropriate.

1. **Shield 1: Strong businesses and citizens**

   Consolidating cyber awareness messages

   We have found that cybersecurity messaging can be fragmented across federal, state, and sector-specific initiatives. For higher education, different forums (e.g. critical infrastructure, research, foreign interference, privacy, cybercrime prevention) often provide overlapping and sometimes inconsistent guidance. We recommend a single authoritative cyber communications framework, co-designed with peak bodies such as AHECS, that tailor consistent messages for students, academics, and other institutional stakeholders.

Increasing cyber literacy in schools and pathways into higher education

Cyber careers must be seeded much earlier in the education pipeline. Although there is a national cyber curriculum, uptake across schools vary. Many schools, particularly in regional areas, lack basic IT classes and cyber awareness training. Early intervention is crucial to shape, establish interest and introduce to underrepresented demographics (i.e. with a focus towards increasing female, indigenous, regional and lower socio-economic student opportunities). As digital pervasiveness amongst society increases, embedding digital resilience and curiosity about cyber in primary and secondary education will build the future pipeline into higher education and, ultimately, the national cyber workforce. The AFP re_B00TCMP program is phenomenal for teenagers and youth offender prevention, but further activities and a wider demographical remit, particularly towards primary school age students, will create the avenue for increased cyber literacy.

Protecting individuals (students and staff) as digital citizens

Universities are not only institutions but communities comprising hundreds of thousands of students, staff (professional and academic), and various industry stakeholders many of whom may be in transitional or vulnerable stages of life. Students are high-frequency targets for scams, account takeovers, and identity theft, often with limited awareness of digital self-protection. Staff and various stakeholders are frequent phishing and social engineering targets, with their individual accounts serving as entry points to broader institutional compromise.

We recommend that Horizon 2 include a focus on building individual cyber resilience. This could include nationally consistent, sector-tailored campaigns, including materials for businesses (and the sector) to include in onboarding and orientation programs, and support for identity protection measures, improved authentication adoption incentives, and recovery assistance for compromised individuals. Personal cyber safety should be embedded into wellbeing and student support frameworks, recognising cyber harm as both a security and a pastoral care issue. Equity and inclusion are critical. Measures must explicitly support First Nations students and staff, regional and remote communities, international students and vulnerable groups, ensuring cyber resilience is not unevenly distributed across society.

Digital literacy programs should include practical skills in detecting scams, protecting online accounts, and securing personal devices which the sector can integrate into university curriculum and staff training. These measures not only reduce the risk to individuals but also strengthen institutional and national

resilience, recognising that whilst the human layer is often the most targeted entry point, humans are also the first responders and greatest strength when informed and united.

Regulatory/compliance requirements and maturity impacts

Universities face overlapping compliance regimes: SOCI Act obligations, Privacy Act reforms, foreign interference guidelines, APRA-like controls (for superannuation/finance divisions), various state-based obligations and international frameworks required by research partners (NIST, ISO, ISM). This complexity diverts scarce cyber workforce resources away from uplift activities into compliance reporting, lowering overall maturity.

We also note the rigidity of AQF-regulated training pathways act as a barrier to rapidly evolving cyber workforce needs. Policies need to adapt more quickly to reflect technological change, new threat actor behaviours and emerging industry requirements. We recommend Government endorsement of an appropriate sector-wide higher education cyber framework, which considers the openness of the university ecosystem and potentially harmonises Essential 8, ISM, and NIST with a proportionate risk informed baseline.

Ransomware and cyber insurance

Universities are prime ransomware targets due to high-value research and sensitive student data. Cyber insurance is increasingly unaffordable and inaccessible, with providers requiring high baselines that few universities can consistently demonstrate. We recommend the Government review and lead a pathway to resolve this increasingly challenging issue. Government supported reinsurance pools or risk-sharing schemes, like terrorism insurance models, to stabilise the cyber insurance market would support not only the Higher Education sector but others more widely.

Supply chain risk

A cybersecurity program is often only as secure as the vendors and service providers it relies on. There is an opportunity to synchronise third-party and supply chain cyber risk management across the nation using a collaborative, scalable approach. Through an agreement between CAUDIT and TMU (Toronto Metropolitan University), the sector currently utilises a collective third-party risk management and benchmarking services which brings 35 Australian and New Zealand universities, and the 200 Canadian universities together within a shared platform where institutions can access benchmarking data,

continuous monitoring, and vendor risk assessments, while leveraging volume purchasing and cost efficiencies. This model reduces duplicated effort across institutions and lifts the overall baseline. Rather than every institution independently assessing common suppliers, a shared service enables coordinated assessments, risk ratings, and control expectations, which are then utilised for local risk decisions. This approach achieves cost efficiency, consistency, and improved leverage in negotiations with suppliers.

We recommend that the Government support and consider scaling this type of collaborative supply chain assurance model across the nation, potentially through grant funding or shared services incentives. This could also serve as a model for other critical infrastructure sectors, such as health and local government, where diverse entities rely on overlapping third-party ecosystems. Government endorsement and alignment with federal supplier risk frameworks (e.g. PSPF, ISM) would strengthen its applicability and ensure integration with broader national supply chain security initiatives.

2. Shield 2: Safe technology

Emerging technologies and wearables

Higher education institutions are at the frontier of adopting mixed reality, smart glasses, and wearable devices for teaching, research, and varied discipline training (such as healthcare). Current frameworks do not explicitly capture these devices. We recommend expanding standards for emerging technologies in education and research, including wearable mixed-reality devices, ensuring alignment with existing IoT and edge device security standards. This should include vendor assurance requirements, given the sector's exposure to foreign-supplied research technology.

AI presents both a productivity opportunity and a disruptive threat. This has cascading implications for both cyber workforce design and baseline digital literacy. Horizon 2 should explicitly consider how the sector can support AI guardrails and support the development of education for rapid uplift to raise cyber and AI literacy across all disciplines. We also recommend clarity on the sector's role in shaping regulatory guardrails for AI security and safety (as a required differentiator from AI governance), as this intersects directly with research, workforce, and national security. Quantum computing is rapidly approaching and will likely impact during this strategy. The government should proactively lead providing guidance, support and guardrails to ensure the sector and Australia more broadly are investing to benefit securely as quantum amplifies both the opportunity and risk.

3. **Shield 3: Threat sharing and blocking**

The higher education sector has a strong track record in collaborative threat intelligence sharing. For example, the AHECS Information Sharing and Analysis Centre (ISAC) is a dedicated threat intelligence sharing group for universities and research institutes managed by the Australian Computer Emergency Response Team (AUSCERT). The AHECS ISAC uses AUSCERTs Malware Information Sharing Platform (MISP) platform, which is a threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

Adoption of threat intelligence can be uneven across institutions. The sector has been reviewing the existing sector ISAC function and model and would recommend support similar to the Health-ISAC initiative (including seed, as well as establishment funding), to extend dedicated support for a similar Higher Education ISAC under Horizon 2, ensuring universities and research institutes have direct access to real-time threat sharing and national blocking initiatives. We also encourage the Government to consider support for development of safe harbour for vulnerability disclosure and bug bounty programs, enabling researchers to responsibly test and report vulnerabilities without fear of legal exposure.

4. **Shield 4: Protected critical infrastructure**

While SOCI has brought much-needed focus to critical infrastructure, the current obligations present challenges in the higher education context, where institutions are complex, federated, and globally interconnected. The legislation is difficult to operationalise, with unclear expectations for what constitutes 'critical' in research. Additionally, regulatory burden risks divert attention from uplift.

We recommend that the Government undertake a sector-specific SOCI regulatory review with AHECS and Universities Australia, and provide templated risk management programs for universities, aligned to SOCI, to reduce compliance duplication. We would also welcome the expansion of Government support with tools, incentives, and co-funding for uplift, rather than compliance-only enforcement.

5. **Shield 5: Sovereign capabilities**

Cyber workforce

The higher education sector is uniquely placed to grow Australia's cyber workforce through teaching, reskilling, and research. The cyber workforce starts at early primary level to foster skills that are aligned

with the future workforce and attract more into the field as they grow and develop. Addressing this at an early age, increases the talent pool of a skilled sovereign community. We would welcome funding of workforce transition pilots targeting underemployed PhD graduates, ex-defence personnel, and transferable skilled and disciplined professionals moving into cyber roles. We believe that Australia could leverage transferrable skillsets from engineering, law enforcement, social sciences, and healthcare for cyber incident response.

We recommend Commonwealth-funded sponsorship of security clearances for students and graduates, removing barriers to entry where eligibility is misinterpreted as requiring an existing clearance. This would unlock access to critical workforce pipelines.

Research and innovation

Universities are Australia's largest R&D, innovation and entrepreneurial engine, yet cyber research funding is fragmented. We recommend establishing a National Cyber Research and Innovation Fund with priorities jointly set by Government, industry, and academia. This would provide stable, long-term funding for both offensive and defensive security research, bug bounty development, and sovereign start-ups. This should be complemented with Commonwealth-supported platforms for kinaesthetic cyber learning (cyber ranges, CTFs, enclaves) that are available across institutions and potentially sectors.

6. Shield 6: Resilient region and global leadership

The higher education sector plays a frontline role in regional engagement through student mobility and research partnerships. We think there is opportunity to leverage universities as trusted channels for Pacific cyber capacity-building and research partnerships under the Cyber Rapid framework. Universities have unique APAC footprints through offshore campuses and partnerships. Horizon 2 should explore leveraging this presence to build cyber capacity across the region, both offsetting domestic workforce shortages and strengthening Australia's reputation as a trusted partner.

We also would support more academic voices included in cyber diplomacy forums on standards, norms, and regulation.

The higher education sector is both a critical infrastructure operator and a sovereign capability builder. AHECS strongly supports the Horizon 2 ambition but stresses that success will depend on:

- harmonising regulation to reduce compliance burden.
- strengthening research and workforce pathways through long-term investment.
- recognising higher education's unique risks such as ransomware, cyber insurance, and emerging technologies.
- embedding universities as partners in international cyber resilience efforts.

We welcome the opportunity to continue collaborating with Government on co-designing sector-specific measures to ensure universities can fulfil their dual role as both resilient operators and national capability builders. Thank you for the opportunity to provide feedback on Horizon 2. If you would like further information, or to explore any of our recommendations or comments, please contact:

[redacted]