THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

The University of Queensland's submission to the Horizon 2 Public Discussion Paper

About UQ

As one of Australia's premier learning and research institutions, The University of Queensland (UQ) is renowned nationally and internationally for the quality of its teaching and research, ranking in the top 50 universities globally. It also hosts the Australian Cyber Emergency Response Team (AusCERT), which is Australia's pioneer cyber emergency response team that helps its corporate members prevent, detect, respond to, and mitigate cyber security incidents.

UQ Cyber Research Centre (UQ Cyber) is an interdisciplinary research centre with a multi-dimensional team of over 60 academics and researchers across various disciplines from the School of Electrical Engineering and Computer Science, TC Beirne School of Law, UQ Business School, and AusCERT, to bring an interdisciplinary approach. From secure quantum communications to researching policies addressing the global cyber security skills shortage, UQ Cyber conducts interdisciplinary research and partners with international organisations to address the biggest challenges facing cyber security around the world.

UQ Cyber has been committed to working to develop cyber and digital resilience in a range of ways. UQ's Master of Cyber program is the first interdisciplinary cyber security program in Australia with four fields of studies, and a new degree that is aligned to the National Institute of Standards and Technology's internationally recognised Cyber Security Education framework, taught by leading academics and industry professionals, with a truly inter-disciplinary approach to the field. The mission of UQ Cyber is to address global cyber security challenges and educate top cyber security leaders.

UQ Cyber has the capability of delivering bespoke cyber training through tailored short course programs, masterclasses, regional dialogues, Master of Cyber Security Studies, and Higher Degree by Research (PhD and Master of Philosophy by Research) programs. We have delivered short courses for leadership that is extremely beneficial for enhancing cyber security capabilities of local governments.

Education: UQ is the pioneer of Australia's first Masters of Cyber program that adopted the NIST cyber security risk management framework, appealing to students internationally. UQ is the first to teach interdisciplinary cybersecurity. All students at master's level are accepted from any degree, so students do not necessarily require a computer science degree (it is a noncognate degree). All enrolled students are brought together as an interdisciplinary cohort with diverse experience (foundations), then they branch into four specialisations. **Cyber Defence**, is where they learn how to defend networks and systems. **Cyber Leadership**, is where they learn how to train current IT leaders to become cyber leaders, on how to make uniformed decisions, and teach best practices and recommended decisions. **Criminology, or cyber criminology** is how to train people who apply crime prevention techniques into preventing cyber-crime. **Cryptography** is how we apply different techniques and engineer the secure solutions. Students finish with a capstone program which students can finish in their home country should they wish.

Expertise: UQ Cyber's interdisciplinary research spans across over 60 experts and their respective research teams across various disciplines who are globally renowned, and offers diverse capacity building capabilities to tackle cybersecurity challenges https://www.cyber.uq.edu.au/team/uq-cyber. UQ researchers regularly contribute to critical vulnerability disclosures in partnership with industry leaders. Notably, UQ Cyber is proud to have reported the highest number of Common Vulnerabilities.

Cyber Security Testing Labs: UQ Cyber is the only university in Australia with a multipurpose living lab setting us apart (Energy Test Lab for hardware physical cyber testing, Device Testing Lab for software cyber security testing, Agile Security Operations Centre + 2 Cyber War Rooms) for real-life testing and cyber-attack and defence exercises.

100+ partnerships: UQ Cyber has many public and private sector partners.
https://www.cyber.uq.edu.au/engage

AUSCERT – UQ has its own (and Australia's first) CERT (Cyber Emergency Response Team) that holds corporate trainings, tabletops for C-level execs, threat intelligence services, and most of all known for its annual industry led AUSCERT Conference (1000+ppl attendance) https://conference.auscert.org.au/

Outreach and Events

UQ Cyber is passionate about raising our community's cyber security posture and have a strong track record of partnering with both public and private sectors to enhance capability and awareness around cyber security, data privacy and cyber affairs. We work with a diverse range of groups - from high school students to government leaders across the Asia Pacific. In addition, UQ have been working with IDCARE on the DFAT Pacific Cyber Resilience Project to provide Specialist Community Support Service Trial for Community Members and Microbusinesses Impacted by Cybercrimes and Online Scams in Papua New Guinea and Fiji since Aug 2024.

UQ is also providing joint national cybercrime support services with IDCARE under the Australian Government Small Business Cyber Resilience Service program since Nov 2024. The small business cyber resilience services are based out of UQ Cyber Agile Security Operations Centre at UQ's St Lucia campus.

Table-top Security Exercises and Workshops

UQ Cyber researchers and professional staff have extensive experience in providing exercises to support ministerial meetings, educational and outreach activities. These include: table-top security exercises and scenarios; mission simulations; engineering cyber ranges and IoT cyber security scenarios as well as workshops for high school teachers and STEM students.

Computer Emergency Response Teams (CERTs)

Our researchers and professional staff have a strong record of partnering with INTERPOL, APNIC, and Pacific Island nations' CERTS and governments to enhance cyber incident response capability, cyber crime prevention, and best practice use of technology to support economic growth and sustainable development in the Indo-Pacific Region. UQ's own AusCERT provides services to members not just from all Australia sectors, but also members from the government, banking and educational sectors across Papua New Guinea, New Zealand and Vanuatu. AusCERT provide training and events for cyber security professionals.

UQ's Cyber Awareness Campaigns and building a Cyber Champions Community:

Since 2022, UQ via its Cyber Culture Team has been proactive in building a community of Cyber Champions, to raise awareness of cyber security and build a strong cyber culture within our organisation, as we are aware that the humans are the weakest link. Our Cyber Champions Network is a community of UQ people who foster a proactive, engaged, and security-conscious ecosystem at UQ. Starting with four founding members, our membership has now grown to 180+ and have received calls from industry to help build the same. If there is a strong need to support non-UQ communities to establish Champions Networks and similar initiatives including those involving training and mentorship UQ team can support. It has supported other organisations such as RACQ in starting their Cyber Champions Networks and we frequently get requests to share best practices from industry and government affiliated bodies.

Executive Summary

This submission to the Horizon 2 Public Discussion Paper compiles feedback from academic and professional staff from the University of Queensland, and includes UQ Cyber Research Centre, UQ Research and Innovation, UQ School of Mathematics and Physics, UQ School of Electrical Engineering and Computer Science, UQ T.C. Beirne School of Law, UQ Business School, UQ Centre for Policy Futures and UQ Information Technology Services division (ITS) (including AusCERT).

This document focuses on specific questions relating to Shield 1, 2, 3, 4, 5 and 6 in the Discussion Paper.

A summary of our recommendations is provided below. Our detailed responses to the six shields are provided in the remainder of the document. Where applicable, our responses relate to specific questions or, in some circumstances, our responses address entire shields.

Overall Recommendations

Recommendation 1: To ensure Horizon 2 delivers visible uplift, we suggest providing twice-yearly public dashboard reporting progress on the evaluation model.

Shield 1 Recommendations

Recommendation 2: We suggest embedding cyber security awareness and education in the education system through collaboration and coordination with State Governments, i.e. through the Commonwealth Government providing resources or support.

Recommendation 3: We suggest tailoring content and delivery of existing campaigns to reach different Australian citizens.

Recommendation 4: We suggest providing a free baseline with a companion checklist in plain language, with a recommended order of operations, to turn awareness into action for SMBs.

Recommendation 5: We suggest providing SMBs and the public guidance on ‘what to expect’ from providers and their responsibilities around cyber security.

Recommendation 6: We suggest that the Commonwealth Government should recognise and leverage existing programs and initiatives across the ecosystem relating to cyber awareness, training and mentorship to uplift the cyber security capability of the ecosystem.

Recommendation 7: Using industry bodies, we suggest developing customised support and resources by industry.

Recommendation 8: We suggest creating a single navigation page mapping government programs, guidance and contacts to make it easy for SMBs to find the right help.

Recommendation 9: We suggest developing a simplified SME and NFP-appropriate version of ASD Essential 8 to leverage existing IRAP and E8 ecosystem and structures.

Recommendation 10: Instead of going down the voluntary standards or certification route, we recommend Australia to introduce legislative reform into existing or new laws to require nationwide cybersecurity principles along the lines of Workplace Health and Safety legislation. This will effect nationwide change, reduces criminal motivation to target Australia, and leverages the existing justice system without the need to create new standards or certification organisations.

Recommendation 11: We suggest implementing funding and other interventions that support and encourage NFPs’ compliance with ASD Essential 8.

Recommendation 12: Provide resources to help NFPs become cyber secure.

Recommendation 13: We suggest collaborating with industry, including insurance associations, to develop SMB-accessible insurance resources including bundling insurance with compliance programs and piloting programs tying incentives to control implementation.

Recommendation 14: We suggest implementing legislative measures that prescribe and enforce cyber maturity levels for SMBs

Recommendation 15: We suggest providing funding and support to help SMBs comply with above-specified requirements.

Recommendation 16: We suggest providing an "obligation map" showing the obligations arising for organisations from relevant cyber security legislation and regulations.

Shield 2 Recommendations

Recommendation 17: We suggest that funding and support be provided to research initiatives to formally verify the security of edge devices, CER and operational technology.

Recommendation 18: We suggest that any technology standards and frameworks developed for accreditation purposes should embed continuous assurance to ensure that the technology remains secure despite evolving threats.

Recommendation 19: We suggest implementing security labelling for IoT devices in a similar system to the Energy Rating used for appliances.

Recommendation 20: We suggest introducing secure-by-default supplier conformance labelling for SME configurations.

Recommendation 21: We suggest forming cross-industry consortiums for SMBs to share intelligence, benchmarking, coordinated mitigation strategies and sharing of supplier cyber risk assessments.

Recommendation 22: We suggest the Government develops frameworks around managing vendor relationships.

Recommendation 23: We suggest that increased funding is devoted to research and development to boost innovation and economic prosperity.

Recommendation 24: We suggest software bills of materials where appropriate are encouraged.

Recommendation 25: We suggest that model contract clauses for logging, data residency and breach notification are provided to industry.

Recommendation 26: We suggest developing accessible and tailored guidance relating to quantum computing and cryptography aligned with NIST's post-quantum cryptography timelines, NIST Cybersecurity Framework 2.0 and ENISA guidance.

Recommendation 27: We suggest providing guidance and training, potentially linked to the Privacy Act Amendments in 2025, relating to the use of AI.

Shield 3 Recommendations

Recommendation 28: We suggest that a software security rating system is implemented similar to the ANCAP safety rating.

Recommendation 29: We suggest that IoT device security labelling is implemented.

Recommendation 30: We suggest increasing the oversight of telecommunications security through a refresh of the legislation.

Recommendation 31: We suggest requiring routers to have filters for traffic, approved by the Commonwealth Government.

Recommendation 32: Establish a single national threat-blocking service that combines government, CERT and major platform signals to distribute product-mapped indicators via DNS, email and endpoint controls.

Recommendation 33: We suggest that ISACs should be proactively created by, first, clarifying the information sharing approach and, second, developing an approach suitable for the Australian context.

Recommendation 34: We suggest that incentives need to be provided to SMBs relating to vulnerability disclosure programs, such as linking these programs to insurance or funding bug bounty programs.

Recommendation 35: We suggest establishing a national vulnerability disclosure program with a safe harbour, a simple intake portal, and a public directory of participating organisations.

Recommendation 36: We suggest devoting funding to spreading awareness about vulnerabilities leveraging existing programs where possible.

Shield 4 Recommendations

Recommendation 37: We suggest that support should be provided to enable critical infrastructure owners and operators to implement Protective DNS and similar controls that require minimum investment and maximum benefit.

Recommendation 38: We suggest that there is greater liability, including personal liability, through legislation placed on directors to encourage better engagement with government security requirements.

Recommendation 39: We suggest that a single navigation point be provided that maps domestic guidelines and requirements, such as PSPF, ISM and SOCI, with reusable artefacts provided.

Shield 5 Recommendations

Recommendation 40: Similar to the US NIATEC initiative, we suggest that there is value in establishing such a collaboration leveraging universities to help grow industry-ready cyber workforce more rapidly through increasing accessibility and industry relevance of university education enabled by injection of funding.

Recommendation 41: We suggest that funding should be provided for stackable and credible micro-credentials mapped to specific roles (e.g. analyst, incident coordinator, operational technology defender), which are recognised by government in recruitment and procurement.

Recommendation 42: We suggest funding and resources should be provided for a structured internships and returnship scheme co-funded with industry, which includes supervised workplace learning and clear conversion targets**.**

Recommendation 43: We suggest that incentives should be provided to the market to encourage organisations to develop incident response capability to improve redundancy in the market.

Recommendation 44: We suggest that support should be provided to expand outreach programs for females in cyber security.

Recommendation 45: We suggest that research translation support and funding should be provided to allow developers and organisations to pilot their products in SMEs, small departments or scoped areas within government to help organisations improve their products and develop sovereign capabilities.

Recommendation 46: We suggest funding should be made available for mid-career transitions to cyber security. As many of these individuals will have families, the funding should cover dependents to properly support the individuals enforcement or intelligence gathering.

Shield 6 Recommendations

Recommendation 47: We suggest that a similar approach could be leveraged in the broader Southeast Asia and Pacific region across law enforcement agencies.

Recommendation 48: We suggest that regionwide joint intelligence and response exercises be conducted with partners and ecosystems.

Recommendation 49: We suggest two-way secondments be initiated between Australian agencies and CERTs, and regional partners.

Recommendation 50: We suggest that the feasibility of hosting data centres or laying additional submarine cables should be explored.

Recommendation 51: After responding to a cyber incident, Cyber RAPID team members should train, at least, 2 individuals in the affected country to uplift the cyber security capability of the country.

Recommendation 52: We suggest that the Commonwealth Government nominates and supports Australian experts to lead work items in priority standards bodies (e.g. ISO/IEC, ITU-T, FIRST).

Recommendation 53: We suggest that domestic cyber security guidance should be reviewed and aligned with industry standards, such as NIST's Cybersecurity Framework 2.0 and other related efforts, e.g. ENISA.

Recommendation 54: Enable an Asia-Pacific forum of universities for research collaboration, training and mentorship.

Shield 1: Strong businesses and citizens

5. What could government do to better target and consolidate its cyber awareness message?

- We acknowledge and celebrate the effectiveness of current federal cyber awareness campaigns (Act Now. Stay Secure). To further build on this effective campaign, we suggest there may be value in incorporating cyber security awareness in the education system, which is supported by research[1].
- We also suggest that there may be a need for tailored content and delivery of the existing campaigns, e.g. through radio and television shows. Bada et al. (2019)[2] illustrate how campaigns should be tailored to the context, specifically, the cultural context. This content should help them know what they can do to be more cyber aware and protect their data in plain language.
- **Recommendation 2:** We suggest embedding cyber security awareness and education in the education system through collaboration and coordination with State Governments, i.e. through the Commonwealth Government providing resources or support.
- **Recommendation 3:** We suggest tailoring content and delivery of existing campaigns to reach different Australian citizens.
- It may also help to provide SMBs with a checklist in plain language, with a recommended order of operations, to help them turn awareness into action.
- **Recommendation 4**: We suggest providing a free baseline with a companion checklist in plain language, with a recommended order of operations, to turn awareness into action for SMBs.
- It may also be helpful to communicate to SMBs and the public 'what to expect' from providers while clarifying the responsibilities of the SMB and the public.
- **Recommendation 5:** We suggest providing SMBs and the public guidance on 'what to expect' from providers and their responsibilities around cyber security.
- Furthermore, UQ is host to an excellent Cyber Champions network with currently over 180 members across the university. Cyber Security Champions are UQ staff who are advocates and volunteer their time to raise cyber security awareness in their area, such as Human Resources, Finance or Student-facing areas. We have observed significant value and traction from these initiatives as there are more individuals passionate about cyber security. Similar Networks are run across Australia with much success, e.g. the Cyber Security Champions of Tomorrow in Brisbane.
- There is a current need from industries for these Networks and similar initiatives including those involving training and mentorship. UQ has supported other organisations in building their own Cyber Champions Networks, e.g. RACQ, and frequently get asked about how we run ours from industry and government affiliated bodies. Hence, further awareness about such initiatives and programs would enable more of these to develop, which would lead to more advocates for cyber security uplifting Australia's cyber security. The Commonwealth Government can also leverage these initiatives and programs by sharing information or collaborating with existing program deliverers to spread cyber awareness and knowledge.
- **Recommendation 6:** We suggest that the Commonwealth Government should recognise and leverage existing programs and initiatives across the ecosystem relating to cyber awareness, training and mentorship to uplift the cyber security capability of the ecosystem.

[1] See Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon, 5*(12).
[2] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour*?.

7. How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance, etc.)?

- Our work with industry has demonstrated the value felt from the existing cyber resources, such as the Small Business Cyber Resilience Service and Cyber Wardens. Largely, our feedback from industry has illustrated that these resources have been effective in establishing baseline cyber security awareness and support. This may include time-boxed, subsidised 'light' assessments aligned to the baseline, producing short remediation plans rather than lengthy reports.
- To further improve uptake of resources, the feedback received indicates that there is demand for customised support and resources for organisations by industry. These customised support and resources will allow organisations to further uplift their cyber security. We suggest that, through collaboration with industry bodies, industry-stratified customised support and resources can be developed helping specific industries to uplift their cyber security.
- **Recommendation 7:** Using industry bodies, we suggest developing customised support and resources by industry.
- To avoid information overload, there is a need to create a single navigation page mapping government programs, guidance and contacts to make it easy for SMBs to find the right help.
- **Recommendation 8:** We suggest creating a single navigation page mapping government programs, guidance and contacts to make it easy for SMBs to find the right help.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?

- While cyber security standards have a place for enterprises and global alignment of best practices, we would like to propose that standards and their certifications are ineffective for resource-tight SMBs and NFPs. Laws are not optional, while standards – at least in the eyes of SMBs – are optional. However, for SMBs and NFPs, standards, which are voluntary, are less effective.
- Fundamentally, having 'yet another' standard or certification would be an impose on them and their customers. Instead, we believe that legislative updates would be a better lever of behavioural change and effective national rollout. We believe that existing legislations such as the Cyber Security Act or Privacy Act's APP 11 could be updated to explicitly make company directors and owners liable for negligent or poor cyber practices. This is also simpler to implement, leverages the existing justice system, longer lasting, and is a truly national uplift like the Workplace Health and Safety (Model WHS Act) legislation.
- Currently, there are numerous duplicated frameworks (e.g., ASD Essential 8, CIS Controls) and standards (e.g., ISO/IEC 27001) already in the market, and there is no reason why we need to reinvent the wheel. If standards are to be developed, we believe that the current ASD Essential 8 is the best basis to work from, since it would just need a minor adjustment to the standard and related processes to make it more accessible to the context of SMBs and NFPs. To ensure ongoing relevance, regular consultation with the stakeholders in the relevant sectors would enable the adjusted standard to keep pace with the latest threats. A regular (e.g. quarterly), minor adjustment/update of Essential 8 is the fastest and least-costly option and least invasive way to align to more comprehensive frameworks such as the ISM and pace with the latest cyber threats.
- Furthermore, as the ASD Essential 8 (and its existing ecosystem such as IRAP assessors) are already being used by the defence and other industries, using it as a standard allows for consistency and coherency across Australia.
- We are aware that there are currently some companies in the industry which are self-touted 'standards bodies' for SMBs. In truth, these so-called 'standards bodies' are not accredited by JAS-ANZ or equivalent bodies and are profit-driven endeavours where both standards body and certification bodies are for-profit companies owned and operated by the same entrepreneurs.
- Worse, the robustness, integrity and assurance of the certification requirements and self-attestation processes of these so-called standards does not assure or guarantee a stronger cyber resilience for SMBs and for Australia. The 'certifications' are in essence a marketing platform for SMBs and NFPs to be exposed to expensive IT and security products and services under the guise of tools helping these SMBs obtain a 'certification' badge – a mirage and a false sense of security for the SMBs without actually addressing the core of the problem in a cost-effective way.
- Cyber criminals do not care about organisations with badges or certificates, since they are empirically proven to be opportunistic. In fact, many breached organisations with resources happen to be certified to standards, so by inference, the 'standards and certification' approach will not work for lesser-resourced SMBs and NFPs.
- The most effective way for SMBs and NFPs to uplift their cyber resilience as a nation would be to utilise the lever of legislative reforms (e.g., making directors accountable for poor or negligent cyber practices; drafting principles in legislation focusing on strong authentication, risk management and incident response best practices), like the effective legislation of Australian workplace health and safety laws in recent years.
- **Recommendation 9:** We suggest developing a simplified SME and NFP-appropriate version of ASD Essential 8 to leverage existing IRAP and E8 ecosystem and structures.

- **Recommendation 10:** Instead of going down the voluntary standards or certification route, we recommend Australia to introduce legislative reform into existing or new laws to require nationwide cybersecurity principles along the lines of Workplace Health and Safety legislation. This will effect nationwide change, reduces criminal motivation to target Australia, and leverages the existing justice system without the need to create new standards or certification organisations.
- Principles and obligations should be proportionate to organisational size and risk, with phased adoption and clear low-cost pathways for SMBs.

10. What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

- NFPs typically face two key challenges: limited budget for indirect costs, such as cyber security[3], and the current regulatory framework does not fully support NFPs' cyber uplift.
- To address these challenges, we suggest interventions should build compliance through "carrots" rather than "sticks. These "carrots" may include providing funding to support compliance with the ASD's Essential 8.
- **Recommendation 11:** We suggest implementing funding and other interventions that support and encourage NFPs' compliance with ASD Essential 8.
- In addition, resources should also be provided to help NFPs establish secure configurations and develop their cyber security maturity easily. Two resources that may be useful are 'secure-by-default' configurations and step-by-step hardening guides for common NFP stacks (email, endpoint and identity) reducing NFPs' burden.
- **Recommendation 12:** Provide resources to help NFPs become cyber secure.

11. Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

- We consider that cyber insurance products are not easily affordable or accessible for small entities. Research[4] has shown that there is limited awareness and understanding of cyber insurance products not helped by the complexity of insurance documentation or the fears around whether cyber loss is covered. There is also a lack of integration between cyber insurance and cyber security frameworks.
- To improve the affordability and accessibility of cyber insurance products for SMBs, we suggest developing training and documentation with simplified language, visual aids and modular policy approach oriented to SMBs. Cyber risk quantification tools could also be employed to assist understandability as these tools, such as calculators and self-assessments, can make abstract risks more tangible.
- We also suggest that, working with insurance associations, insurance could be bundled with compliance programs, e.g. the Essential 8, to encourage adoption.
- An additional program that could be run with insurance providers is piloting premium incentives tied to completion of a baseline security defined by a set of controls, e.g. phishing-resistant MFA and immutable backups.

[3] See Philanthropy Australia's report - https://www.philanthropy.org.au/about-us/publications/paying-what-it-takes-funding-indirect-costs-to-create-long-term-impact/
[4] See Actuaries Institute (2024) for example - https://content.actuaries.asn.au/resources/resource-ce6yyqn64sx3-2093352434-54003

- **Recommendation 13:** We suggest collaborating with industry, including insurance associations, to develop SMB-accessible insurance resources including bundling insurance with compliance programs and piloting programs tying incentives to control implementation.

17. Which regulations do you consider most important in reducing overall cyber risk in Australia?

- We support the use of legislation and regulation to reduce the overall cyber risk in Australia.
- Legislation with punitive consequences for cybercriminals demonstrates the cost of targeting Australian organisations and individuals. Thus, the presence of such legislation reduces the attractiveness of Australian organisations and individuals for cybercriminals.
- We suggest that legislation and regulation targeting organisations should enforce certain levels of cyber maturity while also providing relevant funding and support for SMBs to alleviate the burden and barrier for SMBs.
- One resource that could be provided is an "obligation map" showing clearly the obligations arising from SOCI, Privacy Act and sector rules.
- **Recommendation 14:** We suggest implementing legislative measures that prescribe and enforce cyber maturity levels for SMBs
- **Recommendation 15:** We suggest providing funding and support to help SMBs comply with above-specified requirements.
- **Recommendation 16:** We suggest providing an "obligation map" showing the obligations arising for organisations from relevant cyber security legislation and regulations.

Shield 2: Safe technology

18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

- While there are international best practice examples available, we would like to direct attention to the Australian-developed seL4 Microkernel[5] . Its security has been formally verified, and it is currently in used by the US and UK military. Yet, its usage in Australia is limited to the best of our knowledge. Following the seL4 example, we suggest that one approach to enhancing secure edge devices, CER and operational technology is using formal verification to confirm security. This may be enabled through funding and support of research initiatives.
- **Recommendation 17:** We suggest that funding and support be provided to research initiatives to formally verify the security of edge devices, CER and operational technology.
- Furthermore, any use of secure technology standards and frameworks for accreditation purposes should recognise that security is not a static concept considering the dynamic threat landscape. There is a need to embed continuous assurance in any standards and frameworks to ensure that the technology deemed secure is still secure despite evolving threats.
- **Recommendation 18:** We suggest that any technology standards and frameworks developed for accreditation purposes should embed continuous assurance to ensure that the technology remains secure despite evolving threats.

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

[5] See https://sel4.systems

- Currently, we observe that it is difficult for consumers and end-users to be aware of the cyber security of their products. Considering the success of the Energy Rating used for appliances, such as washing machines and dryers, we consider there is benefit in using a similar system for security.
- Specifically, we suggest upfront labelling for IoT device security could be used for the hardware (as the software changes) following research[6]. A similar system could be implemented with the support of the Commonwealth Government.
- **Recommendation 19:** We suggest implementing security labelling for IoT devices in a similar system to the Energy Rating used for appliances.
- Similar secure-by-default supplier conformance labelling could also be introduced for SMB configurations, e.g. for MFA on by default, hardened administrative access and logging enabled.
- **Recommendation 20:** We suggest introducing secure-by-default supplier conformance labelling for SME configurations.

20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

- Foreign ownership, control or influence risks associated with technology vendors are relevant to all organisations, irrespective of size. Larger organisations may be well-suited to managing these risks. However, for SMBs, managing these risks may create administrative burdens.
- To support smaller organisations, we suggest, with the support of government, cross-industry consortiums could be formed to enable shared intelligence, benchmarking, coordinated mitigation strategies and sharing of supplier cyber risk assessments. We note that the sharing of assessments may be appropriate as the well-regarded Department of Home Affair's Foreign Ownership, Control, or Influence Risk Assessment Guidance for procuring technology products or services can take 60-90 minutes. Sharing results can ease the administrative burden for SMBs.
- **Recommendation 21:** We suggest forming cross-industry consortiums for SMBs to share intelligence, benchmarking, coordinated mitigation strategies and sharing of supplier cyber risk assessments.
- The Commonwealth Government could also build on the aforementioned Assessment Guidance by developing frameworks to support the due diligence, transparency and accountability in vendor relationships. This may include providing guidance tailored to specific concerns, such as geopolitical risks.
- **Recommendation 22:** We suggest the Government develops frameworks around managing vendor relationships.

22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed or exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

- Boosting innovation and economic prosperity requires investment into research and development. Ongoing research and development through stakeholders, such as universities, is necessary to ensure Australia remains protected while the threat environment evolves.

[6] See Shen, Y., & Vervier, P. A. (2019, June). Iot security and privacy labels. In Annual Privacy Forum (pp. 136-147). Cham: Springer International Publishing.
Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020, May). Ask the experts: What should be on an IoT privacy and security label?. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 447-464). IEEE.

- **Recommendation 23:** We suggest that increased funding is devoted to research and development to boost innovation and economic prosperity.
- Furthermore, there may be value for secure innovation if software bills of materials where appropriate are encouraged, and if model contract clauses for logging, data residency and breach notification are provided to industry.
- **Recommendation 24:** We suggest software bills of materials where appropriate are encouraged.
- **Recommendation 25:** We suggest that model contract clauses for logging, data residency and breach notification are provided to industry.

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

- There are two emerging technologies where guidance is critically needed: quantum computing and artificial intelligence (AI).
- The potential threats arising from the emerging technology of quantum computing and its impact on cryptography, such as the 'harvest credentials now, decrypt later' criminal mentality, means that it is critical for guidance to be provided to raise awareness. Our experience has indicated that awareness about the potential issues is low and tends to be concentrated in specific areas within a country. There is a need to increase awareness and accessibility to such knowledge.
- Guidance should be aligned with the global industry, e.g. NIST's post-quantum cryptography timelines, NIST Cybersecurity Framework 2.0 and ENISA guidance, to avoid any Australian unique-divergence.
- **Recommendation 26:** We suggest developing accessible and tailored guidance relating to quantum computing and cryptography aligned with NIST's post-quantum cryptography timelines, NIST Cybersecurity Framework 2.0 and ENISA guidance.
- Guidance and training are needed for AI as there are a number of security risks that may affect organisations and individuals, e.g. non-malicious insider threats, data-related vulnerabilities, cybersecurity and privacy breaches, data input manipulation and AI hallucinations. The risk of biased datasets not helped by limited transparency in model development and training data sources can also compromise the inclusiveness of decisions made using AI models. Relevant guidance could link to the Privacy Act Amendments in 2025 relating to automated decision-making processes to encourage ethical and transparent use of AI.
- Furthermore, the Government could also encourage transparency in AI development and vendor diversity.
- **Recommendation 27:** We suggest providing guidance and training, potentially linked to the Privacy Act Amendments in 2025, relating to the use of AI.

Shield 3: World-class threat sharing and blocking

24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

- Similar to the ANCAP safety rating system, we suggest a similar approach can be implemented relating to software security. Such a system encourages industry to be more proactive about the security of their developed software to move from 1 star to 5 stars.

- **Recommendation 28:** We suggest that a software security rating system is implemented similar to the ANCAP safety rating.
- We also suggest that for IoT devices, as referenced in our response to Question 19, there may be value in using device labelling. The US is initiated labelling for consumer IoT devices[7]
- **Recommendation 29:** We suggest that IoT device security labelling is implemented.

26. How could government further support industry to block threats at scale?

- Malicious traffic flows through telecommunications networks meaning that increasing the security responsibility and obligations of telecommunication providers can be a scalable mechanism to protect Australia.
- **Recommendation 30:** We suggest increasing the oversight of telecommunications security through a refresh of the legislation.
- Considering the issues with the security of routers, we suggest that routers should be tagged with filters by default, which will filter traffic. Another approach can be requiring the password change of routers.
- **Recommendation 31**: We suggest requiring routers to have filters, approved by the Commonwealth Government.
- There is also a need to provide a single national threat-blocking service that combines data from government, CERT and major platforms to distribute product-mapped indicators via DNS, email and endpoint controls. This will aid threat-blocking at scale.
- **Recommendation 32:** Establish a single national threat-blocking service that combines government, CERT and major platform signals to distribute product-mapped indicators via DNS, email and endpoint controls.

27. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

- There is a need to form ISACs proactively however the formation of ISACs is limited by the lack of clarity, awareness and literacy on how to share data. As an example, we consider the US Presidential Decision Directive 63[8], which introduced guidelines on ISACs and the public-private partnership relating to information sharing. A similar approach is recommended to clarify the sharing of information between government, industry and academia. The chosen approach should consider previous efforts and the Australian context working with CERTs.
- **Recommendation 33:** We suggest that ISACs should be proactively created by, first, clarifying the information sharing approach and, second, developing an approach suitable for the Australian context.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?
32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

- There is a need for a vulnerability disclosure program. For SMBs, it can be difficult to implement these programs. One approach could be to link these programs to cyber insurance. Another approach is to provide funding for organisations that establish vulnerability disclosure programs similar to a bug bounty program.

[7] See https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0
[8] See https://irp.fas.org/offdocs/pdd/pdd-63.htm.

- **Recommendation 34:** We suggest that incentives need to be provided to organisations relating to vulnerability disclosure programs, such as linking these programs to insurance or funding bug bounty programs.
- Further, for SMBs, there may be benefit in establishing a national vulnerability disclosure program with a safe harbour, a simple intake portal, and a public directory of participating organisations. Such a program would allow SMBs to easily adopt vulnerability disclosure programs without bespoke legal work.
- **Recommendation 35:** We suggest establishing a national vulnerability disclosure program with a safe harbour, a simple intake portal, and a public directory of participating organisations.
- While there are CVE Numbering Authority systems for the Common Vulnerabilities and Exposures (CVE) discovered, additional work is needed to spread awareness about vulnerabilities. Rather than a government-centred program, we suggest that the Commonwealth Government could instead direct attention to existing programs, e.g. Monah University – Cyber Security Incident Response Team is now a CVE Numbering Authority
- **Recommendation 36:** We suggest devoting funding to spreading awareness about vulnerabilities leveraging existing programs where possible.

Shield 4: Protected critical infrastructure

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

- Our experience has shown that there is a need for controls to be selected for organisations requiring minimum investment and maximum benefit. One control is Protective DNS. According to Infoblox (2025)[9], 92% of malware attacks would be reduced if Protective DNS was enabled.
- **Recommendation 37:** We suggest that support should be provided to enable critical infrastructure owners and operators to implement Protective DNS and similar controls that require minimum investment and maximum benefit.

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

- While we acknowledge that there is some awareness in private sector partner about the importance of cyber security requirements, we suggest that the lack of board awareness may cause cyber security requirements to not be taken more seriously. Considering how workplace health and safety are treated seriously due to the Workplace Health and Safety Act, we suggest that ensuring directors are more liable for cyber security may help.
- **Recommendation 38:** We suggest that there is greater liability, including personal liability, through legislation placed on directors to encourage better engagement with government security requirements.
- There also needs to be greater clarity between the different domestic guidelines and requirements to support organisations in compliance and implementation.
- **Recommendation 39:** We suggest that a single navigation point be provided that maps domestic guidelines and requirements, such as PSPF, ISM and SOCI, with reusable artefacts provided.

[9] Infoblox. (2025). Infoblox for Protective DNS. Retrieved from https://insights.infoblox.com/solution-notes/infoblox-solution-note-infoblox-for-protective-dns.

Shield 5: Sovereign capabilities

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots, or policy ideas do you think would best support industry to grow?

- The US's National Information Assurance Training and Education Centre (NIATEC) is a consortium of organisations including universities, industry and governments focused on improving the awareness, comprehension, teaching and education of Information Assurance in the US.
- **Recommendation 40:** Similar to the US NIATEC initiative, we suggest that there is value in establishing such a collaboration leveraging universities to help grow industry-ready cyber workforce more rapidly through increasing accessibility and industry relevance of university education enabled by injection of funding.
- Furthermore, similar to the UK's Academic Centres of Excellence in Cyber Security Research, we suggest that research centres can be established in universities to allow further research innovation and excellence.
- The development of an industry-ready workforce should be prioritised using government-recognised stackable micro-credentials mapped to specific roles, and structured internships and returnships co-funded with industry with set outcomes.
- **Recommendation 41:** We suggest that funding should be provided for stackable and credible micro-credentials mapped to specific roles (e.g. analyst, incident coordinator, operational technology defender), which are recognised by government in recruitment and procurement.
- **Recommendation 42:** We suggest funding and resources should be provided for a structured internships and returnship scheme co-funded with industry, which includes supervised workplace learning and clear conversion targets.
- To further aid the development of the cyber workforce, it may be appropriate to decentralise cyber security in terms of incident response. Currently, there are only a limited number of organisations that can be used for incident response. If there were incentives for other organisations to develop the relevant talent for incident response, this will embed redundancy into the market.
- **Recommendation 43:** We suggest that incentives should be provided to the market to encourage organisations to develop incident response capability.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM fields more broadly?

- We note the success of existing outreach programs, such as the UQ-ASD engagement programs to schools focused on female students. Additional support could be provided to expand these outreach programs in Australia and the Pacific region.
- **Recommendation 44:** We suggest that support should be provided to expand these outreach programs.

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

- We note the concentration of cloud infrastructure and AI technology providers in the US. Such concentration may limit the competitiveness and innovation while negatively affecting the inclusiveness of the technology. To combat this international reliance, which may negatively affect the sovereign capability of Australia, we suggest that initiatives be implemented to encourage Australia-based capability and innovation. Australia can then capitalise on first of the world research.

- **Recommendation 45:** We suggest that research translation support and funding should be provided to allow developers and organisations to pilot their products in SMEs, small departments or scoped areas within government to help organisations improve their products and develop sovereign capabilities.
- As inclusiveness and diversity is critical for innovation, we suggest that support and resources should be devoted to easing the transition for mid-career individuals into cyber security through scholarships and other funding to help the individuals retrain in cyber security. This may include extending such funding to the Pacific to allow for Australia to contribute to building the cyber security capacity of the Pacific.
- **Recommendation 46:** We suggest funding should be made available for mid-career transitions to cyber security**.** As many of these individuals will have families, the funding should cover dependents to properly support the individuals enforcement or intelligence gathering.
- With the emerging technology of post-quantum computing and its implications for cryptography, there is a need to increase awareness as the risks of not using appropriate solutions may be detrimental (see our response to Question 23). Our experience has indicated that awareness about the potential issues is low and tends to be concentrated in specific areas within a country. There is a need to increase awareness and accessibility to such knowledge. We repeat the recommendation from Question 23 (Recommendation 26)

  Recommendation 26: We suggest developing accessible and tailored guidance relating to quantum computing and cryptography aligned with NIST's post-quantum cryptography timelines, NIST Cybersecurity Framework 2.0 and ENISA guidance.

Shield 6: Strong region and global leadership

46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

- We consider that sanctions are effective tools for countering growing malicious cyber activity.
- Further tools could be considered but require rigorous research and evaluation before being employed.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

- We applaud the Australian participation in the Pacific Islands Law Officers' Network and the success of this initiative in improving the security in the Pacific communities through its responsiveness compared to treaty-based initiatives.
- **Recommendation 47:** We suggest that a similar approach could be leveraged in the broader Southeast Asia and Pacific region across law enforcement agencies.
- Furthermore, these efforts should extend to conducting joint intelligence and response exercises with partners and ecosystems in South-East Asia and the Pacific to uplift the broader security and incident response capability of the region.
- **Recommendation 48:** We suggest that regionwide joint intelligence and response exercises be conducted with partners and ecosystems.
- In addition, there would be benefit in encouraging two-way secondments between Australian agencies and CERTs and regional partners to support the capability uplift within the region.

- **Recommendation 49**: We suggest two-way secondments be initiated between Australian agencies and CERTs, and regional partners.
- Following the comments from Tech Council of Australia and Atlassian co-founder Scott Farquhar, there is capacity for Australia to host data centres for the Southeast Asia and Pacific region providing a way for Australia to enable the security of the Pacific while leveraging the cost and other advantages that Australia possesses.
- Additional submarine cables could also be laid to improve connectivity and resilience, considering the Tongan undersea cable was damaged causing two islands to be without internet after an earthquake[10].
- **Recommendation 50:** We suggest that the feasibility of hosting data centres or laying additional submarine cables should be explored.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

- While the Cyber RAPID team has been incredibly effective in responding to cyber incidents, to provide further value to the Pacific region, we suggest that the team after responding to the incident, should train two individuals in the affected country for each RAPID staff sent before departing.
- Sharing knowledge and training Pacific individuals will empower and increase the capability of Pacific states in a sustainable way, uplifting the cyber security of the overall region in the long run.
- **Recommendation 51:** After responding to a cyber incident, Cyber RAPID team members should train, at least, 2 individuals in the affected country to uplift the cyber security capability of the country.

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

- Currently, the market is risk-based leading to a lack of transparency as the individual determines and responds to their perceived risk.
- The government can improve transparency through the reforms listed above and encouraging regional collaboration and enabling innovation.
- The government should leverage academics to represent Australia in standardisation bodies beyond ISO/IEC, for example ITU-T. The government could also consider nominating experts and providing secretariat support to the strategic global standardisation efforts of these academics.
- **Recommendation 52:** We suggest that the Commonwealth Government nominates and supports Australian experts to lead work items in priority standards bodies (e.g. ISO/IEC, ITU-T, FIRST).
- To complement the strategic global standardisation efforts mentioned above, we suggest that there should be greater alignment between any domestic guidance, e.g. the ASD's Essential 8, and NIST's Cybersecurity Framework 2.0 and efforts from ENISA.
- **Recommendation 53:** We suggest that domestic cyber security guidance should be reviewed and aligned with industry standards, such as NIST's Cybersecurity Framework 2.0 and other related efforts, e.g. ENISA.
- As a university, we suggest that significant value and innovation can be delivered through a regional forum of universities across the Asia-Pacific region led by Australia to share research and insights, collaborate, and provide mentorship and training. We encourage government grants and investments catalysing Australian-Pacific university research collaborations. This will support the

[10] See https://www.theguardian.com/world/article/2024/jul/16/parts-of-tonga-without-internet-after-cables-damaged-and-starlink-ordered-to-cease-operations.

uplift of the innovation and overall security capability of Australia, and the research capabilities and security of the Asia-Pacific.

- We note that university Chief Information Officers are already in a similar forum, but are currently missing the coverage of research training and research capacity building.
- **Recommendation 54:** Enable an Asia-Pacific forum of universities for research collaboration, training and mentorship.

Contributors' List (Alphabetical Order)

[redacted]

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Contact details

uq.edu.au

cyber.uq.edu.au

auscert.org.au

CRICOS Provider 00025B •