AUSCERT

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

12 April 2023

Discussion Paper
2023-2030 Australian Cyber Security Strategy

UQ CYBER and AUSCERT

Joint submission

The University of Queensland
Brisbane QLD 4072 Australia
E cyber@uq.edu.au
W uq.edu.au

ABN: 63 942 912 684
CRICOS Provider 00025B
TEQSA PRV12080

Contents

Executive Summary

UQ Cyber and AusCERT welcome the opportunity to provide the present submission to the Discussion Paper released by the Expert Advisory Board on how government can achieve its vision under the 2023-2030 Australian Cyber Security Strategy. The Strategy represents a major opportunity for Australia to build on its reputation as the number 1 country in the world in terms of progress and commitment to enhancing cyber security. Despite the significant, recent data breaches that have affected Australian organisations and residents, the way forward in our quest to become the most cyber safe country in the world should be one of optimism. The Strategy has the potential to be a 'guiding light' in this journey.

Since the start of their operations, UQ Cyber and AusCERT have built a solid partnership, putting the pair at the cutting edge of cyber security education, research, and practice. Grounded in a truly multi-disciplinary approach, combining subject matter expertise in virtually all the disciplines contributing to comprehensive cyber security ('horizontals'), and the functional activities involved in 'full stack' cyber security ('verticals'), our work leverages collaborative efforts involving academia, industry and organisations, government as well as individuals.

We believe the Strategy should adopt this very same collaborative approach, and be a document that unites, not one that divides. Striking a delicate balance between national sovereignty and need for agility, the Strategy should address the needs of large corporations as well as small and medium enterprises. Its initiatives should uplift the understanding of, and proactive engagement with, cyber safe practices for all residents at the individual level, so to shape a broader cyber secure society.

A technical document with clear goals and methods to measure their achievement, more than a simple declaration of intents, the Strategy should be a living artefact, and cater for the rapid changes that the ever-evolving cyber-threat landscape requires. Increased collaboration in the Pacific and APAC regions, harmonisation of the current regulatory frameworks, coordination of agencies' efforts in strengthening cyber security and increasing cyber resilience are some of the key areas we recommend the Strategy focuses on. These, and several others, are put forward in the present submission, which addresses the Discussion Paper as a whole, and each question raised by the Expert Advisory Board in it.

For further information, we are available at:
cyber@uq.edu.au

About UQ Cyber

At UQ Cyber, we are proud to be one of the first universities in the world with a truly interdisciplinary approach to the complex challenges of cyber security. UQ has been a pioneer in cyber security since 1992. UQ Cyber builds on the traditions of UQ's AusCERT which was established in 1992 as the second oldest computer emergency response team after Carnegie Mellon University's pioneering establishment of its CERT/CC.

Since the establishment of the UQ Cyber centre in February 2019, through a university-wide strategic initiative involving almost all faculties and schools, a centre and an institute, we have a strong interdisciplinary team which has been consistently featured as one of the top institutions of choice for cyber security learning and research in the APAC region.

Our 50+ researchers and practitioners are regularly trailblazing frontiers in cyber security and data privacy research, are published in the top journals and conferences across the fields of computer science, software engineering, power and electrical engineering, quantum physics, social sciences, criminology, political science, policy studies, psychology, law, economics, management, auditing, governance risk and compliance, and information systems.

We value diversity of thought and backgrounds, and intentionally designed our NIST NICE-aligned Graduate Certificate, Graduate Diploma and Master of Cyber Security programs to take in students from any Bachelor degree. All Master of Cyber Security students graduate with a capstone project working on either research projects or an industry placement. UQ Cyber also features the highest number of CVEs reported for any Australian university and contributes to several critical vulnerability disclosures to our partners.

Our graduates are in high demand in the industry, and several of them receive job offers before they finish their degrees. Since its establishment in 2019, students from our elite student club, the UQ Cyber Squad, have been regularly featured amongst the top three positions across all cyber competitions (e.g., National Shearwater Challenge, Cyber 9/12) in Australia and around the world. We are also hosts of the Oceania Qualifiers of the International Cybersecurity Challenge (i.e., the 'World Cup' of cyber security competitions).

With cutting-edge facilities such as the Industry 4.0 Energy TestLab, Agile Security Operation Centre, Device Testing Lab and Cyber War Rooms to support learning and research, we strongly believe that we are creating the best environment for interdisciplinary cyber security research and education.

https://www.cyber.uq.edu.au/

About AusCERT

At AusCERT, we're passionate about data security and keeping your information safe. That's why we deliver 24/7 service to our members alongside a range of comprehensive tools to strengthen your cyber security strategy.

From the start of AusCERT, we've continued to develop our systems and our culture to be the best it can be. Our range of services accommodate all areas of network security for your organisation. Our culture will be the reason you love us though. If you're looking for a CERT or for a company that really gets you, you're looking in the right place.

Our company was founded over 25 years ago when a university student hacked NASA in his spare time. This breach triggered a chain reaction for improving information security. In the early 1990's three Australian Universities came together and formed AusCERT – the central source for information security and protection. Today, The University of Queensland (UQ) has embraced AusCERT as part of their organisation.

https://auscert.org.au/

SECTION A - General feedback

Recent cyber-breaches: The Discussion Paper (DP) acknowledges that in the spate of significant cyber-breaches occurred during the months of September-October 2022 in Australia, the government was ill-prepared: this is a good starting point to building cyber resilience from the ground up. The DP reflects on the importance of national sovereignty, which is well posited, and mirrors a trend that characterises policy-making efforts by other countries around the world.

National sovereignty: National sovereignty and centralised cyber security need to be balanced with consideration of the highly fragmented and 'asymmetric' nature of the cyber-landscape, and how this will likely evolve in the future. The gap in required resources between attackers and defenders is likely to widen further; at the same time, transnational, collaborative efforts in the field of cyber security seem to call for a 'no-boundary' attitude with regards to information and best practice sharing in cyber-defence. Further, recent data breaches indicate the importance of strengthening data security at the individual level. The concepts of national sovereignty and decentralised defences are not mutually exclusive: the Strategy needs to cater for both.

Australia in the Pacific and beyond: The DP stresses the importance for Australia to work with regional partners in uplifting cyber resilience in the Pacific. The Department of Foreign Affairs and Trade (DFAT) has recently promoted a series of initiatives in the field of security, covering both the physical and the digital sides[1]. These can be taken as a foundation for enhanced collaboration in cyber security in the region. The Strategy needs to emphasise the importance for Australia to keep focusing on securing the Pacific through alliances with countries in the area, with a view to subsequently broaden this approach to include the whole Asia-Pacific region (APAC).

Frameworks harmonisation: The '*Enhancing and harmonising regulatory frameworks'* section of the DP covers a crucial aspect of what the Strategy will need to do. On this note, the Strategy should be crafted to cover the needs of large, as well as medium and small organisations (SMEs). The latter are often the ones struggling the most with understanding what cyber security regulations apply to them and how to comply.

Agencies alignment: On a similar note, harmonisation is also needed across government cyber security agencies and departments, at both the State and the Federal level. To avoid misaligned, or worst, conflicting views, guidelines, and recommendations, or unclear messages, communication channels need to be strengthened among agencies and between agencies and recipients: individuals, organisations, and society in general. The DP does not seem to address this issue and the Strategy should be more explicit on this.

Cyber Resilience: The DP mentions cyber security and cyber resilience as synonyms, when they're not. The Strategy should illustrate, for the plain reader, the differences, mainly revolving around the assumption, through cyber resilience, that protection from all attacks is virtually impossible and emphasising the need to complement preventative efforts with investments in

[1] https://www.dfat.gov.au/geo/pacific/shared-security-in-the-pacific

response and recovery, two areas in which Australian organisations, in general, have traditionally been lagging behind.

Goal setting and performance management: The DP does not refer to how the performance of the Strategy will be measured: considering that the current Australia's Cyber Security Strategy 2020 is silent on this point too, it is envisaged for the new Strategy to be more technical and explicit: clear goals will need to be set, as well as details on key performance indicators, performance measurement and management processes, etc.

Timeframe: The Strategy is expected to cover the time span 2023-2030. In cyber security terms, this is a very long time. The ever-changing threat landscape requires agility in terms of capacity for adaptation, customisation, and re-design. The Strategy should be flexible enough to cater for regular monitoring and review.

SECTION B – Specific questions

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

- Practical actions aimed at helping Australia build stronger capabilities in cyber security, through both increased numbers of graduates in cyber security programs and better trained cyber-professionals.

- Concrete initiatives for SMEs: the regulatory framework surrounding their operations is likely going to become more complex, putting further pressure on them; regulatory requirements need to be complemented with resources towards compliance (e.g., grants, mentoring services and other support).

- Measures towards strengthening Australia's role in facilitating cooperation at the regional level, with a view to build a cyber-secure Pacific through collaboration.

- Concrete initiatives aimed at building cyber resilience in Australia and its region. This can be achieved by increasing efforts in the phases of response and recovery, two areas in which the country has been lagging. The proposed creation of a National Office for Cyber Security within Home Affairs is a step in the right direction but needs an accompanying strategy. Australia houses one of the oldest running Computer Emergency Response Teams (CERT) in the world; New Zealand itself has a very efficient and functioning CERT. Cyber resilience in the Pacific (and APAC overall) could significantly benefit from these. Australia's military tradition can be very helpful in shaping a national culture of ability to effectively respond to cyber-crises and bounce back from them.

- Maintaining significant investments in automation to improve the country's ability to prevent cyber-breaches, fostering a collaborative approach among industry, government, and academia to this purpose.

- Harmonisation between proposed amendments to the *Privacy Act 1988 (Cth)* and any legislative amendments considered under the Cyber Security Strategy, as strong privacy laws encourage investment in cyber security[2].

- Steps towards the development of a 'brand' over the next few years for cyber safe Australia. According to MIT's annual Cyber Defence Index[3], Australia ranks #1 in the world in terms of collective cyber security assets, policy stances, and organizational capabilities, with the latter having the lion's share. It is fundamental for the new Strategy to leverage this and propose practical actions to 'market' Australia's capabilities in this field.

[2] Impact_of_GDPR_on_cyber_security_outcomes.pdf (publishing.service.gov.uk)
[3] The Cyber Defense Index 2022/23 | MIT Technology Review

- Whilst controversial, Australia needs to ensure there exists a strong 'disrupt and dismantle' element to its strategy, *à la* the US Cyber Security Strategy[4]. The Australian Signals Directorate (ASD) already possesses a legislative mandate to conduct disruption operations against overseas operators, and this should be called out in the Strategy. Domestically, the lead and support roles of Australia's national security agencies should also be clarified.

2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

- Over the years, numerous regulatory instruments have been enacted that are aimed at carefully managing the inevitable risks associated with the development of the digital economy. In some areas, redundancies may have emerged (e.g., critical infrastructures), whilst in others there could be need for further regulation (e.g., SMEs). Whatever the approach adopted by the Strategy will be, it represents the first significant opportunity towards a clarification of existing legislative and regulatory instruments, to consolidate/simplify where necessary, before considering new legislation (if, and where needed).

- At the same time, re-organising legislation or drafting entirely new policies will not be sufficient, if adequate communication to the recipients is not guaranteed. In the presence of scarce resources (e.g., for smaller organisations or individuals), simply hoping for entities to abide by regulations is wishful thinking. Anecdotal evidence from industry and organisational partners suggests they would welcome further practical guidance on 'how' they can comply with the law.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

- Legislative instruments such as the *Security of Critical Infrastructures Act 2018 (Cth) (SOCI Act)* constitute a significant step forward in clarifying obligations around cyber security and, ultimately, protecting Australia's most valuable assets. However, regulations are not sufficient in isolation. Australia needs to enhance its capacity to build capabilities in the field of critical infrastructures, by developing professionals specialised in their protection (e.g., multi-disciplinary teams of subject matter experts, with a variety of backgrounds in terms of experience, abilities, and culture) and enabling those managing the infrastructure to fully comply with their legal obligations.

- From a customer's perspective, one may question why customer data held by a critical infrastructure provider should be treated differently by the law compared with customer data held by a non-critical infrastructure provider.

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

- The *SOCI (CIRMP) Rules (LIN23/006) 2023* already capture critical data storage or processing assets as defined by section 12F of the *SOCI Act*[5]. Extending the reach of the definitions would arguably capture every business or commercial entity holding customer data and 'systems', unless the definition was extremely specific (and would then arguably lose its application). An alternative would be to indicate that the customer data held by entities already covered by the SOCI is also subject to the Act – i.e., by using the definition of 'business critical data' already in the Act to capture information held by critical infrastructure.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

- The current general perspective is that boards' existing obligations of care and diligence and of acting in good faith and in the company's best interest (*Corporations Act 2001 (Cth),* ss 180-184[6]) already cover and include cyber-risk oversight. This seems confirmed by the *SOCI Act*, which calls for an all-hazard approach when it comes to boards' responsibility for risk oversight, including cyber-risks. Further, leading institutions in this field (e.g., the Australian Institute of Corporate Directors - AICD) seem to maintain that further legislative clarification, especially in terms of directors' personal liability in case of sub-optimal oversight on cyber-risks, is not required.

- On the other hand, recent research has shown that some board members (especially those working for companies not listed in the Australian Securities Exchange market (ASX) or organisations not covered by legislative instruments from the Australian Prudential Regulation Authority (APRA)), have asked for further clarity on their obligations and liability in oversight of cyber-risk[7]. On this note, legislation worldwide seems to push in the direction of making boards' responsibility in cyber security more explicit: the US Securities and Exchange Commission, for example, has proposed in March 2022, among others, the obligation for companies of a certain size to disclose cyber security expertise among their board members[8]. Several analysts have drawn parallels between the aforementioned proposal and the *Sarbanes-Oxley Act* twenty years before, which required expertise and disclosure at the board level, in the field of financial reporting[9].

- Effective support in helping board directors discharge their duties in terms of cyber-risk oversight is likely to come from a mix of different actions, mainly aimed at uplifting board members' skills and expertise in the field of cyber-risk management. Directors do not need to become experts in technical cyber security, but they do need to be comfortable with discussing how cyber-risks could impact their organisations, and what to do in case of a successful cyber-attack. Directors should also have practical guidance from government which set out 'how' organisations can comply with their legal obligations.

[5] https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure/regulatory-obligations
[6] https://www.legislation.gov.au/Details/C2017C00328
[7] Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cyber security from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, 121, 102840.
[8] https://www.sec.gov/news/press-release/2022-39
[9] Zukis, B., 2022. The SEC Is About to Force CISOs Into America's Boardrooms. *Forbes*: https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/?sh=41f8771268a9

- To achieve this, the Strategy should identify practical opportunities for cyber security training and awareness programs aimed at directors, involving constituencies of subject matter experts such as industry, academia, government, and corporations. A particular focus should be placed on improving collaboration around desktop simulations and crisis management exercises for boards of Australian organisations to learn how to respond to, and recover from, cyber-breaches.

- Finally, one may question why board obligations regarding cyber security risks be specifically called out when other risks and issues (climate change, workplace bullying, underpaying staff) are not.

d. Should Australia consider a Cyber Security Act, and what should this include?

- Other legislation and laws, including the common law, cover cyber security issues. Typically, new legislation creates new rights and obligations; changes (overrules or replaces) existing rights and obligations; or codifies existing laws. At present, there does not appear to be a major gap in the law that needs to be legislated regarding cyber security. Similarly, there does not appear to be any existing law or practice regarding cyber security that needs to be overruled.

- It has been suggested that allowing the practice of 'hacking back' should be legalised. Legislation was proposed in the United States,[10] but this has not progressed. Existing legislation (such as the *Intelligence Services Act 2001 (Cth)*) already permits such activity against offshore actors; however, the legal position is unclear if aimed at a computer or network located in Australia. If legalised, hacking back should be conducted by the government under strict supervision and Ministerial/judicial oversight, not by private citizens or businesses.

- Laws regarding prohibiting the payment of ransomware or reporting the payment of ransoms have also been suggested, and there was a Bill proposed in 2021 that is reportedly not proceeding[11]. If such laws are considered appropriate, this alone does not suggest a need for a general *Cyber Security Act*. This is discussed further below in this document.

- If there is any such *Cyber Security Act*, it should focus on supporting and funding the building of cyber security capabilities and cyber security education, and facilitating international cooperation, rather than adding more regulation and red tape.

- Any new law should recognise that absolute cyber security is not possible. As stated by Justice Rofe in *ASIC v. RI Advice Group*: "Cyber security risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible to reduce cyber security risk to zero, but it is possible to materially reduce cyber

[10] The proposed bi-partisan bill called the *Active Cyber Defense Certainty Act (ACDC)*.
[11] *Ransomware Payments Bill 2021*, for further reference, see: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6730

security risk through adequate cyber security documentation and controls to an acceptable level."[12]

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

- The Strategy should include practical steps to support companies of all sizes, with priority for SMEs, in strengthening their cyber security capabilities. This could include public/private partnerships, government grants aimed at SMEs to uplift their cyber security via in-house resources or outsourced services (e.g., Managed Security Services Providers, MSSPs), large-scale reviews of compliance against existing regulations, maturity-based assessments, etc.

- Similarly, the government should commit to regular reviews of the impact of cyber security regulations on businesses, similar to the five-yearly review process in the UK[13].

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances? What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?

- Despite the importance of addressing the criminalisation of payment of ransoms and extortion demands, mechanisms to restrict financial transactions with criminal entities in this space already exist. These mechanisms should be pursued along with monitoring and controls activities, to make sure impact in the Australian context is minimised. The application of financial transaction restriction under the pretext of the pursue of cyber-threat actors is to be treated at a national level in the same way as restrictions enacted to entities that have been assessed to negatively impact the Australian context. Criminalisation of ransomware and/or extortion payments, although seemingly a strong statement, may adversely affect the victims' ability to recuperate (by rights of insurance or other transferral controls) from acts of crime, instead of mitigating the effect of the initial extortion.

- As further elaboration to the point above, education and collaboration to improve the response of individuals, organisations, and society to ransom and extortion requests by cyber-criminals are of crucial importance. By virtue of education and collaboration, knowledge and awareness of ransomware, cyber-extortion, and associated regulations can be uplifted. The Strategy should contain measures to this goal. An example could include the creation of platforms for information sharing on established best practices in the mitigation of adverse consequences from ransomware attacks. Such initiatives should involve a wide user-base, with stakeholders representing the victims, their organisations (e.g., SMEs and larger ones), government entities and consumers' associations.

[12] First Australian court judgments on cyber security (aicd.com.au)
[13] https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review

- Banning ransomware payments would be difficult to enforce, given that most ransomware incidents are not reported to authorities (whether payments are made or not). Indeed, banning such payments would act as a disincentive to reporting.

- Banning insurance coverage for cyber security incidents also poses potential issues by risking 'third party moral hazard', i.e., it creates an incentive for third parties to turn to ransomware as a sure way of extracting funds from insurance companies.

- One possible, alternative proposal involves taking a dual-pronged approach:
    - Corporate 'bailouts or payments tied to a precondition that the firm invests a certain portion of the aid towards more sophisticated recovery systems and better security education of its employees; and
    - The imposition of a tax on ransomware payments rather than banning them, thereby increasing the total amount payable and disincentivizing the overall appeal of recourse to ransomware payments.[14]

- Any limitations on such payments may consider an exemption where payment is needed in a situation involving 'immediate and significant threat to human health or life', i.e., ransomware attacks on a hospital or health facility.

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

- The government already promotes actions that add a criminal element on to the business decision of remuneration of certain entities (see, for example, the Australian Cyber Security Centre's recommendations on ransom payments). Despite anecdotical evidence suggesting that a large number of organisations affected by ransomware do proceed with payments[15], further criminalisation of payments may serve no further purpose.

- On the other hand, clear messages around the repercussions associated with transacting with criminal entities on the basis of ransom or extortion need to be emphasised on a regular basis. More pervasive communication channels and clarification of legal jargon may be very helpful in this sense, in particular for smaller organisations.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

- Australia should work towards the creation of stronger connections with neighbouring countries, with the goal of uplifting the cyber resilience of the Pacific region. The country already has well-established connections with New Zealand, for example, and numerous parallels can be drawn on how the two are currently managing their cyber security (e.g., the role of CERTs). The Strategy should propose measures to strengthen such

[14] https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/551673d1-1749-446f-b9cb-6516b38b3158/content
[15] https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542

connection and expand best practices in the whole Pacific, with a view to include the APAC region as well.

- As an example, cyber response and recovery could be domains for significant investment in the Pacific, leveraging the role of governmental and non-governmental CERTs, Computer Security Incident Response Teams (CSIRTs), Cyber Security Operations Centres (CSOCs) and Information Sharing and Analysis Centres (ISACs).

- The Strategy should contain actions for the creation of regional cyber security excellence centres, where cyber professionals from the Pacific are trained and exchange ideas and information with their peers from other countries.

- Besides the official networks and agencies, the Strategy should also promote the support for existing communities of practice (CoPs) within sectors. These are often 'unofficial' groups (albeit usually supported by employers) and provide excellent reach into many domains. An example for the Higher Education sector is the Australian Higher Education Cyber Security Service (AHECS)[16] and its associated CoPs.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

- As mentioned before, Australia should intensify its efforts in promoting collaboration and partnerships at a regional level first. Recent examples have illustrated how countries in the Pacific have been experiencing the consequences of cyber-attacks, resulting in significant operations downtime and economic losses[17]. At a broader scale, similar events have recently happened in the APAC, which continues to rank as the most attacked region in the world[18].

- Despite the positive impact of operational initiatives such as the Pacific Cyber Security Operational Network (PaCSON), further consolidation of an agreed-upon perspective on an open and safe internet in the Pacific region is required.

- The Strategy should include measures to do so, for example, by:
    - Nurturing a network of well-prepared cyber security professionals through engagement and collaboration with established tertiary education institutions in Australia and across the Pacific; a practical action could be an increase in the number of scholarships offered within the Pacific to expand cyber-capabilities;
    - Enhancing information sharing at the civil-to-civil level, where government entities are reluctant to release information to entities without security clearances (e.g., Negative Vetting Level 1);
    - Promotion and funding for civil-to-civil (non-governmental) exchanges of cyber security tool use and techniques.

- On the global stage, expertise and knowledge acquired at the Pacific level could be leveraged by Australia to maintain its commitment towards becoming a cyber safe nation

[16] https://ahecs.edu.au/
[17] https://therecord.media/guam-telecom-cyberattack-restore
[18] https://www.ibm.com/reports/threat-intelligence

and supporting allies and international partners in doing the same. Similar initiatives could be expanded to involve the whole APAC region as well.

- Recalling that the AUKUS agreement also included closer collaboration between the UK and US on cyber capabilities, Australia's Coordinator for Cyber Security should invoke the AUKUS Agreement to work in conjunction with the UK National Cyber Security Centre (NCSC) and the US Cyber security and Infrastructure Security Agency (CISA).

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

- There are several avenues for Australia to become a proactive contributor in the field of setting international cyber security standards. Considering that protecting end-users from the adverse consequences of data breaches is paramount, one such contribution could be the establishment of a star rating system for the security of Internet-of-Things (IoT) devices, whose market shows no signs of slowing down. Projections demonstrate in fact that internet-connected devices in 2023 could be as many as 43 billion, three times higher than just 5 years ago[19]. A rating system would guide consumers and empower them to make informed consumption decisions, especially with regards to the data and privacy risks associated with such devices. An internationally recognised regime for IoT security based on such a rating system could be practically built based on the Australian Government's 2020 '*Code of Practice: Securing the Internet of Things for Consumers*'[20]. Against this backdrop, Australia could also exercise leadership in promoting effective collaboration in the Pacific region, as mentioned earlier in this document.

- Generally speaking, Australia could boost its role on the global scenario as a proactive player in standard-setting by leading collaborative initiatives involving neighbouring countries and international bodies. Examples in this sense could include making stronger contributions into the activities of sub-committee 27 of the Joint Technical Committee JTC1 of the International Standardisation Organisation (ISO/IEC JTC 1/SC 27 '*Information security, cyber security and privacy protection*')[21], whose main goal is to establish standards for the protection of information and ICT in general. Other avenues for contribution include standardisation bodies of the International Telecommunications Union (ITU-T).

- Besides the establishment of international standards, emphasis should be placed on the importance of education and awareness around such standards, to help recipients (individuals, organisations, and societies at large) maintain compliance.

[19] https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things
[20] See https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf and the 2021 discussion paper https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.
[21] https://www.iso.org/committee/45306.html

6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**

- Two possible suggestions for the government in the space of serving as cyber security best practice are as follows:
    - The first is replicating the success of the FINTEL Alliance in combatting money laundering by creating a similar private-public partnership for cyber security[22]. The FINTEL Alliance consists of representatives from public and private partner organisations that work together to combat complex or emerging crimes impacting the community, which require a joint, public-private approach. The Alliance facilitates the information and analysis sharing of financial intelligence to investigate and disrupt criminal and terrorist activity. Partners in the Alliance collaborate in the Operations Hub (a physical space for the real-time analysis and exchange of financial intelligence, combining data with tracking tools and best-practice methodologies), and the Innovation Hub (where partners co-design and test innovative technological solutions that assist in gathering and analysing financial intelligence at an operational level). A similar model could be replicated for cyber security.
    - The second is leveraging government power in the establishment of cyber security verification processes in a manner similar to what happens in the EU[23]. The European Union Agency for Cyber Security (ENISA) verifies and certifies entities once they meet a particular cyber security standard, if that standard is one recognised by ENISA. This way, ENISA promotes a wide variety of technical standards without unnecessary reliance on a single one, and also permits entities to choose a standard which best suits their business. ENISA may also determine whether or not certification is voluntary or mandatory in any given industry or sector (this requires two-yearly reviews of any such ruling). At the same time, the proposed *EU Cyber Resilience Act*[24] includes requirements for access control, vulnerability assessment, user activity monitoring, cyber resilience, security by design and patch management.

7. **What can government do to improve information sharing with industry on cyber threats?**

- Currently, the way that CERT Australia's organisational structure is set up, under the ASD, makes this unit very cautious about what information it provides. Seeing that there is no longer an expectation of this CERT forking some of itself back to the Attorney General, its nature is not expected to change. At present, there exists an emphasis on the individuals who are sharing information with the CERT to hold an NV1 security clearance at least, in order to be included into any discussion in the context of released Indicators of Compromise (IoCs). It is suggested, to minimise impact to industry, that the highest position that is in charge of information security be NV1. This would greatly help cleared Directors of Information Security, C-suite professionals or equivalent, better understand the context of any IoC communicated by the CERT. Although NV1 is more

[22] Fintel Alliance | AUSTRAC
[23] EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)
[24] EU Cyber Resilience Act | Shaping Europe's digital future (europa.eu)

'intrusive' than a Director Identification Number (Director ID[25]), which is required by the Australian Business Registry Service (ABRS), this could potentially be an effective way for the CERT to be comfortable sharing information. Requiring NV1 at the Director or C-suite levels means that context information is given at the appropriate level in the target organisation. At the same time, the reverse flow of information, from industry to government, usually needs permission at the Director or C-suite levels about types of data that can be released. Overall, having Directors and C-suite individuals in discussion with the national CERT may elicit easier reverse flow of information to the government.

- In addition, a review of the required classification levels of threat and incident information may facilitate better sharing of that information. For example, a list of technical indicators of compromise might not need to be highly classified. The Cyber Threat Intelligence Sharing program (CTIS) by ACSC is an excellent example of this concept, providing threat information to the industry at lower classification levels, whilst still maintaining (to all outward appearances, at least) relevance and appropriate secrecy.

- As an alternative solution, as ACSC is housed within ASD and is part of the *Intelligence Services Act 2001 (IS Act)* agencies, the legislation could be amended (*IS Act*, s 40) to provide tailored exemptions for ACSC to share information in the following circumstances:
    - If it would materially contribute to the prevention or cessation of a cyber incident;
    - If it would materially protect human health or life from imminent or ongoing serious harm.

- Such disclosures would need to be caveated by a rider that they do not contain information which might lead to the identification of a victim-entity, and/or disclosures must not compromise any of the following: current or planned *IS Act* operations; current or planned investigations by law enforcement; and/or methods or techniques used by *IS Act* agencies or law enforcement (similar to *Freedom of Information Act 1982 (Cth*), s 37)[26].

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

- Regardless of whether the perception is improved by obligating confidentiality, the federal government could also leverage existing, trusted systems such as industry ISACs. In some cases, sharing cyber incident information rapidly and to the appropriate recipients might be better executed outside of the government. ISACs are member-driven organizations, that work on delivering information relevant to all-hazards threat and mitigation services to asset owners and operators. The United States started implementing the ISAC model around 1998, by effectively supporting their existence, while leaving their operations to individual industry groups[27].

[25] About director ID | Australian Business Registry Services (ABRS)
[26] https://www.legislation.gov.au/Series/C2004A02562
[27] https://www.nationalisacs.org/about-isacs

- There is a concern that any obligation of confidentiality may lead to unintended consequences. For example, if during an incident, a business only created documents that were provided to ASD or ACSC, and these documents are subject to an obligation of confidentiality, then such documents may not be able to be used for other purposes, such as to develop learnings and training after the event, reporting to other agencies (Office of the Australian Information Commissioner – OAIC; APRA), reporting to shareholders, and in discovery in a litigation. This is already a concern regarding sections 45(1) and 47(1)(a) of the *SOCI Act*. Obligations of confidentiality should not allow businesses to creatively shield relevant information to avoid their other legal liabilities.

- Generally, the UK NCSC has already adopted a similar approach with regards to cyber-incident management[28]. In the *'Working with the NCSC during a cyber-incident'* document[29], it is suggested that "many regulators will view early engagement with the NCSC as a positive factor when considering regulatory responses"; however, there is no empirical assessment of that statement.

- Another consideration would be to suggest provisions in the *SOCI Act* or *Privacy Act* for limited defences in 'safe harbour' situations, i.e., by creating "a legal remedy for cyber-responsible organizations that provides them an affirmative defence to liability caused by data breaches if they implement and maintain a cyber security program that meets an industry-recognized standard and can show compliance at the time of the attack"[30]. However, safe harbour would not be available in cases of negligence or malfeasance. Safe harbour provisions can thereby only shield the corporation from liability related to the data breach and only if they can show proper due diligence to an appropriate technical standard that was in a state of compliance at the time of the attack. This may be on the issue of a 'Ministerial certificate' or similar.

9. Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

- Ransomware has created a new form of monetisation of cyber-crime, one that does not require the involvement of the 'dark web'. For this reason, among others, ransomware attacks are meant to increase in prominence. At the same time, it is worth noting that arguably some public entities are already required to report an attack to the public based on rules by the ASX.

- Current statistics on reported ransomware attacks can be found in the newly restored yearly report by ACSC[31]. The report has a section dedicated to Ransomware as well as statistics of 447 report over the period July 2021 - June 2022. Having a more comprehensive regime for notification may only affect reported numbers, but not reach to the public. The Strategy should embrace an alternative approach, namely better defining what is done with reported events and how these events are communicated to

[28] Incident management - NCSC.GOV.UK
[29] https://www.ncsc.gov.uk/files/NCSC_Incident_brochure.pdf
[30] Cyber security Safe Harbor: What You Need to Know | Fortress SRM
[31] ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

the public for awareness increase. To help with this, where needed, mechanisms to utilise publicly available data (including from 'onion sites') and the media to more effectively disseminate data about the scale and impact of ransomware should be included in the Strategy.

- At the same time, ransomware reporting should also be improved for ease of attribution of future attacks and greater understanding of threat actors and software vulnerabilities. However, the government would need to carefully consider which entities would need to make such mandatory reports.

- It should also be noted that in the US a law was recently proposed (*Ransom Disclosure Act of 2021*[32]), where reputation and stock values were listed as the primary sources of resistance against enhanced reporting obligations.

10. What best practice models are available for automated threat-blocking at scale?

- Best practice models for automated threat-block at scale need to take two complementary approaches: vulnerability protection and vulnerability prevention. The former is important for existing software and third-party software, while the latter is important for new software developed within Australia, possibly in collaboration with international partners.

- To protect against vulnerabilities in existing software, a key issue is detection accuracy and speed of dispersion of the information about newly detected vulnerabilities. This requires a well-supported Australian Cyber Threat Intelligence (CTI) database and organisation to ensure that intelligence (tactical, operational, or strategic) about new vulnerabilities is filtered, prioritised, and propagated to Australian organisations quickly so that high-risk vulnerabilities are fixed with minimum delay. Reducing the detection accuracy or the speed of dispersion will impede the effectiveness of the effort in harvesting and publishing the CTI.

- To prevent new vulnerabilities being created by Australian software developers, key strategies include promoting the use of automated static analysis tools, safe programming languages, and security formal verification systems that can guarantee freedom from certain kinds of vulnerabilities. For example, SQL injections and buffer overflows (two of the most common vulnerabilities) can be completely eliminated by using appropriate libraries and checking tools. Australia needs to develop or adopt a certification or rating system to encourage the adoption of software developed with such security guarantees so that Australian organisations and individuals who are purchasing software can consider the cyber-security quality of software as part of their purchasing decisions.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

- Despite its affinity with other STEM disciplines and functions, cyber security is unique in that it entails the presence of an adversary, requiring professionals to often adopt an

[32] H.R.5501 - 117th Congress (2021-2022): Ransom Disclosure Act | Congress.gov | Library of Congress

'adversarial' approach when designing appropriate defensive mechanisms. For this reason, a tailored approach, possibly involving cohorts of professionals with accumulated experience in general security (involving, for example, physical security and risk management, e.g., the military and/or veterans) is very much required to upskilling the cyber security workforce, as well as the broader population.

- The Strategy should include consideration of the need for cyber security upskilling in various disciplines. As recently emphasised by numerous delegates at the Pacific Telecommunications Security Expert Forum hosted in November 2022 by UQ, in collaboration with DFAT[33], to best cater for the multi-disciplinary nature of cyber security, skills development should equally focus on technical and non-technical skills (e.g., leadership, change management, policy-making and implementation, law, governance, public relations).

- In this area, again, other countries and supranational unions provide practical examples on how to achieve the goal of implementing a tailored approach for cyber-skills uplifting. As an example, in the EU, ENISA has recently introduced the European Cyber security Skills Framework (ECSF), a practical tool for the identification of required tasks, competencies, skills, and knowledge for cyber security professionals in the Union[34]. The establishment of a similar framework in Australia would be a first step towards clarifying educational and training requirements to strengthen the cyber security workforce in the country. The ASD has created a similar framework, the *'ASD Cyber Skills Framework,'* but uptake has arguably been limited[35].

- Generally speaking, Australia's education system should better encourage pupils towards careers in cyber security, for example by incorporating in current curricula cyber security education. More formalised mechanisms could include the acquisition of Certificates III for graduating year 12 students, for tertiary credit towards a more structured cyber security program in their future.

- Stronger support of cyber security programs in higher education by the federal government would be warranted. Universities currently offering cyber security courses may be more effective if other pressures were to be reduced from teaching staff, allowing greater collaboration with industry to provide feedback loops on the skills required and implementing rapid and more frequent updates to curricula.

- The federal government could also set up 'visibility tools' to know who is doing what in cyber security from an educational (and research) standpoint. ENISA, for example, currently maintains the Cyber Security Education Database (CyberHEAD)[36], a one-stop-shop portal for European citizens looking to upskill in cyber security.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

[33] https://global-partnerships.uq.edu.au/PTSEF
[34] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
[35] https://www.asd.gov.au/careers/resources-hub/cyber-skills-framework
[36] https://www.enisa.europa.eu/topics/education/cyberhead#/

- From an education perspective, the government should play a leading role in facilitating collaboration and engagement among involved stakeholders: industry, higher education, schools, individuals, etc. The components necessary to build, and support, the Australian cyber security workforce are mostly there already; more effective coordination, to avoid redundancies, fragmentation and 'missing links', is what is mainly needed.

- A valid approach to achieve the goal of better coordinating the 'moving parts' tasked with shaping Australia's cyber security workforce of the future is to adopt a 'full stack' approach: the government should act as a supervisor/facilitator, offering tools and mechanisms for the involved stakeholders to aggregate around, and 'do their thing'. As mentioned above, the creation of a cyber security skills framework on the model of the one maintained by ENISA would be an example of this.

- From an immigration perspective, streamlining visa processing and facilitating the immigration of talented cyber security professionals to Australia would be two obvious recommendations. To do so, the government should have a longer-term view of who could become, with support and necessary education or experience, a valid cyber security professional, tapping into the required diversity of backgrounds needed to effectively work in this field. Flexibility in terms of visa conditions and inclusion of cyber security jobs in the skilled occupation lists are two possible measures to this purpose.

- In collaboration with industry partners, the government should also re-consider citizenship requirements for candidates for cyber security job requiring specific clearances. Depending on the context of the profession, ad hoc requirements for application, not necessarily connected to citizenship, may be more suitable, especially considering the gap in cyber security workforce Australia currently suffers from, and the willingness of numerous foreigners to move to the country.

- From an accreditation perspective, Australia should closely monitor initiatives in other countries aimed at professionalising cyber security, with a view to codify skills, experiences, and job attributes for professions in cyber security. On the model of what is currently being proposed in the UK by the Cyber Security Council (NCSC's Certified Cyber Security Professional scheme[37]), which launched a pilot program towards chartership of two categories of cyber security jobs (Governance & Risk Management and Secure System Architecture & Design, with Audit and Assurance and Security Testing to be added), the government should facilitate co-design efforts to shape what such a program could look like in Australia. AustCyber is leading a similar initiative, the Australian Cyber Security Professionalisation program, whose work is currently ongoing[38]: end-users (e.g., professionals who will need to have their professional status assessed and 'certified') must be involved, for co-design to be authentic.

- On this note, the role of the government in maintaining these initiatives focused on 'shaping the greater good' of upskilling cyber security professionals and codifying cyber security jobs will be of utmost importance, in order to avoid professionalisation and associated accreditation mechanisms becoming a private sector revenue stream.

[37] https://www.ncsc.gov.uk/blog-post/the-new-route-for-cyber-security-professional-recognition
[38] https://www.austcyber.com/acsp

- On a conclusive note, the government should support programs that increase diversity (gender, cultural, racial, ability, etc.) in cyber security teams. Increasingly a team effort, rather than an exercise in isolation, cyber security benefits from a range of skillsets, experiences, and background, which is best enhanced through multi-disciplinary, diverse teams. Yet, the cyber security profession has been traditionally characterised by a 'mono-cultural' approach, perpetuating the prevalence of a specific set of technical skills. For example, the number of female professionals in cyber security in Australia is estimated to be around 16% of the total workforce[39]. Governmental measures to increase gender diversity include, but are not limited to, the development of policies to support working women (e.g., day-care support), the reframing of cyber security as a term and an industry in less male-oriented terms, etc.[40]

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

- One of the biggest challenges in this space is the concept of authorising the use of cyber-offensive techniques ('hacking back') inside Australian territory. ASD already has a legislative (*IS Act*) and Ministerial remit to conduct cyber-offensive operations against persons and entities located overseas (even despite the potential issues with foreign sovereignty); however, they lack that authorisation to operate domestically.

- Recent research[41] has identified that the Australian legal framework on domestic cyber-offense is fragmented and conflicted:
    - Australian Federal Police (AFP) officers must obtain a warrant issued by a Judge to 'hack back'; ASD may do so under an instrument issued by the Minister; and the Australian Security Intelligence Organisation (ASIO) requires a warrant from the Attorney-General;
    - The statutes place ambiguous and imprecise boundaries on the lawful mechanism for counter-cybercrime capability to be used in a domestic-threat scenario;
    - The policy parameters under which these activities could be conducted has not been examined or established publicly by any Commonwealth government;
    - There is no publicly available information on the lead agency for a cyber security incident, whether the response conducted is guided by the agency's remit, i.e., 'disrupt and deter' (ASD), 'gather intelligence' (ASIO), 'investigate and prosecute' (AFP);
    - There are further jurisdictional issues between responses by Commonwealth agencies (ASD, ASIO and AFP) and State and Territory police forces (responding to the incident because of complaints or criminal intelligence).

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

[39] https://www.rmit.edu.au/news/ccsri/womens-employment-cyber-security
[40] Women in Cyber - Exploring the Barriers, Redesigning the Profession (uq.edu.au)
[41] Walker-Munro, B., Mount, D., and Ioannou, R., 'The Hacker Strikes Back: Examining the Lawfulness of "Offensive Cyber" under the Laws of Australia' (2023) *Australian & New Zealand Computer Law Journal*, forthcoming.

- A single reporting portal for all cyber incidents is a concept that has undeniable merit. The UK NCSC runs a similar centralised reporting portal[42]. Australia did run something similar in the Australian Cybercrime Online Reporting Network (ACORN) which has now been replaced by ACSC's ReportCyber[43]. The system should be open to law enforcement and *IS Act* agencies at the back end to allow them to be capable of responding to cyber incidents as well as conducting future scanning and post-incident investigations. It should also permit jurisdictional deconfliction, i.e., a state or territory Police Officer should be able to see that the matter is being dealt with by (for example) the AFP, and so not take steps that would interfere or interrupt that investigation. At the same time, given the specificity of cyber-incident reporting for different industries (including underlying reporting obligations), a parallel and joint reporting system organised by industries is also an option.

14. What would an effective post-incident review and consequence management model with industry involve?

- Information sharing requires appropriate guarantees of confidentiality, visibility, and rewards for companies that do decide to share information. A number of incidents in Australia have been showcased as best practice on handling disclosure, such as the Australian National University[44], the Red Cross[45], and most recently Deakin University in 2022[46]. Showcasing these types of incidents as 'responsibly disclosed' may encourage similar good practices, if support is shown by the government in this way. This could provide a reward as an alternative/complement to sanctions such as those already introduced by the government.

- The review of data classifications was mentioned previously in this submission, with the goal of lowering the required classification to enable more rapid sharing of threat data. Naturally, this must be executed carefully to avoid providing adversaries advanced knowledge of cyber defence tactics, but with a more reasonable balance towards assisting Australian organisations with their defence efforts. Also, the government should build upon the existing briefings the Joint Cyber Security Centre (JCSC) holds after incidents. Informal channels could be used to quickly convey declassified information during an incident, rather than waiting until the post-incident review. The JCSC already has a large community via its state-based and national Slack channels. Perhaps declassified, semi-official communications could be made via this channel during incidents, to allow rapid sharing of threat information.

- Referring to the suggestion of safe harbour above, there should be a mechanism for the Minister to provide 'safe harbour' from legal liability to victim-entities which discharge their obligations in good faith and have cyber security protections in place at the time of the cyber-incident.

[42] https://report.ncsc.gov.uk/
[43] https://www.cyber.gov.au/acsc/report
[44] https://www.anu.edu.au/news/all-news/vcs-message-release-of-the-data-breach-incident-report
[45] https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people
[46] https://blogs.deakin.edu.au/deakinlife/2022/07/12/deakin-has-been-targeted-in-a-cyber-attack-this-week-heres-what-happened-and-what-you-should-do/

- Individuals may need specific support (i.e., credit score management and monitoring, document replacement). Coordination and communication around such support (e.g., to promote them, where available) should be facilitated by the government in collaboration with industry players, notwithstanding the latter's obligations in this space.

- Any governmental assistance for victim-entities should be linked back into a need for reinvestment into cyber defences.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

- As a matter of priority (and given the strong technological component associated with cyber security) government, industry, and academia should work together to create programs and initiatives aimed at uplifting technological literacy in the broad Australian population. Setting an appropriate baseline would in fact enable subsequent more effective efforts in upskilling which, as mentioned elsewhere in this submission, is of crucial importance.

- Moreover, the promotion of cyber security awareness (which starts at home), should be paramount. This involves educating people about the risks associated with cyber-threats and how to protect themselves and their families. Individuals should be encouraged to adopt good cyber hygiene practices. The government can work with industry to develop public education campaigns that target a wide range of audiences. These campaigns should emphasise the importance of cyber security, the risks associated with cybercrime, and the steps that individuals and businesses can take to protect themselves.

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- The government has been doing significant work in providing SMEs with free-of-charge tools and instruments to assess their cyber security posture and understand their maturity levels. The ACSC's Small Business Cyber Security Guide[47] or, in a more structured fashion, portions of the ACSC's Essential Eight Maturity Framework[48] applicable to SMEs are two examples in this direction. These initiatives should be complemented with more practical measures that do not entirely rely on the SMEs capacity, availability, and willingness to engage with their cyber security. In this sense, a more comprehensive, proactive approach, in the form of a one-stop-shop platform for all of SMEs' cyber security needs could be an avenue worth exploring. The UK NCSC has recently launched a similar initiative, the Cyber Action Plan[49].

- The Strategy will also need to consider the recommendation contained in the *Privacy Act Review Report* which would remove the small business exemption from the *Privacy Act* itself. This will mean that small businesses (i.e., annual revenue <$3 mil) will be required to comply with the Australian Privacy Principles. Therefore, wherever possible, the

[47] https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide
[48] https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[49] https://www.ncsc.gov.uk/news/ncsc-launches-new-services-help-small-organisations-online

advice of government should achieve both privacy and cyber security requirements from a policy, technical, and practical perspective.

- From a practical viewpoint, as a consequence of the point above, the Strategy should lay the foundations for practical actions to help SMEs in their cyber security uplifting. Examples of such actions (which can be defined in implementation documents and policies following from the Strategy) would include initiatives providing monetary support (e.g., government grants or tax incentives), secondment opportunities with SMEs for graduates or early career professionals, mentoring networks and programs leveraging the expertise of established professionals in the field, etc.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

- There are opportunities for the government to play a stronger position in funding and incubating successful cyber security businesses (e.g., start-ups), whilst increasing sovereign capabilities in the process. Examples include accelerator and incubator programs and funds dedicated to cyber businesses, on the model of what is currently done in other countries (e.g., the US, Canada, Israel).

- There is also a role for the government in increasing the awareness and sophistication of the Australian investor community into backing Australian cyber security companies. Australian investors are traditionally sceptical when it comes to investing in cyber security businesses. Consequently, Australian-based start-ups go abroad and talk to more aware venture capitalists, with the risk of losing them to other markets, which are already more attractive from a talent perspective (e.g., higher salaries, lack of payroll taxes, etc.).

- The government could also explore leveraging research and development funding or tax mechanisms (e.g., reduce payroll taxes for cyber security start-ups and businesses) to catalyse Australian cyber security innovation.

17. How should we approach future proofing for cyber security technologies out to 2030?

- Future proofing for cyber security technologies out to 2030 requires:
    - Encouraging research on improved cyber security practices;
    - Requiring certification or rating systems to ensure that existing best practices for cyber security are adopted and adequately disseminated; and
    - Providing resources to make certification easier.

- The first requirement is to encourage cyber security research by improved research funding, scholarships, and industry tax provisions, so that the skills and knowledge of the Australian cyber security community can be built up, and improved cyber security tools and techniques can be developed. This requirement will be best met by facilitating collaboration among relevant stakeholders, e.g., industry, government, and academia/research institutions. The Strategy should contain practical measures on how to achieve this.

- The second requirement is to develop and promote certification standards and rating systems to encourage the adoption of software that is robust against various kinds of cyber-attacks. A possible option could be an extension of the Australian Information Security Evaluation Program[50] (AISEP) to support a range of certification levels, similar to other systems like the Nationwide House Energy Rating Scheme[51] (NatHERS) star ratings for energy efficiency of houses or the Australasian New Car Assessment Program[52] (ANCAP Safety) ratings for cars. Another valid example in cyber security is the *UK Product Security and Telecommunications Infrastructure Act 2022[53] (PSTI)*, a regulatory instrument that bans 'default' passwords on new connectable devices like smartphones and IoT devices (i.e., those with default 'admin' accounts or having a factory-set and easily guessable password). The *Act* also requires manufacturers, importers, and distributors to comply with security requirements in their goods.

- The third requirement is to provide Australian software developers with resources that enable them to easily adopt such cyber security standards. Such resources could include standardised requirements, test procedures, expected results, and recommended tools that can be easily acquired to perform these standard cyber security tests. Having standard cyber security requirements and providing resources for testing software to check that those requirements are satisfied would allow cyber security technology creators/manufactures to be able to perform the tests before marketing their products. The easier it is for creators and manufacturers to perform tests, the more easily they will be willing to integrate this set of testing minimums as part of the product development process. This suggestion does not include specifically having a product certification, but rather lowering the threshold of performing test. As an analogy, one could think of the Gaming Laboratories International 11: Gaming devices[54] (GLI-11) standard, well-known in the gaming industry. If this standard was accompanied by a guide on how to perform the necessary tests, then the threshold of doing these tests before approaching an accredited certification laboratory would be reduced, resulting in an easier adoption of the GLI11 standard overall.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

- There are numerous opportunities associated with procurement, to use it as a lever to strengthen the Australian cyber security ecosystem. Examples which the Strategy should consider include facilitating the selection of Australian-based cyber security providers over foreign competitors. Besides supporting the Australian ecosystem, such opportunities would also go hand in hand with the expected efforts on national sovereignty and to build a stronger case for promoting local service providers over competitors from abroad.

[50] https://www.cyber.gov.au/acsc/view-all-content/programs/australian-information-security-evaluation-program
[51] https://www.nathers.gov.au/
[52] https://www.ancap.com.au/
[53] https://bills.parliament.uk/bills/3069
[54] https://gaminglabs.com/wp-content/uploads/2018/09/GLI-11-Gaming-Devices-V3-0.pdf

- Whilst controversial, the previous Coalition government published a *Building Code*, which was a Ministerial document which enacted IR regulations for Commonwealth procurement. Entities which did not comply with the Code could not bid for Commonwealth construction work and could be banned from tendering if they were found to be non-compliant.

- A similar opportunity could arise under the Strategy for a *Ministerial Code* (perhaps published under the Rules provision of the *SOCI Act*), which limits Commonwealth procurement of services to those which can meet the one of a set of prescribed cyber security standards. Again, tendering would be prohibited for entities not capable of demonstrating compliance with those standards.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

- Elements for the Strategy to enhance security by design in emerging technologies have been illustrated in the response to question 17 of this submission. It will be worthwhile, however, to emphasise here the fundamental importance of streamlining the process associated with testing products/technologies early. The process could be made more straightforward by listing out test goals and processes, offering insightful explanations on testing techniques, and providing easily accessible tools to conduct the tests.

- The government should identify methods to conduct early tests in close collaboration with technology manufacturers, in order for corrective actions to be applied promptly. Subsequently, a more decentralised system for 'on the spot' testing should be codified, to promote agility in the testing process, for example by involving like-minded individuals and professionals, without the need for dedicated testing laboratories. Follow-up from the results of tests will be crucial, and the government should promote mechanisms for rapid intervention in case of issues identified by such tests.

- Moreover, the Strategy can promote proactive legislation of emerging technologies that establishes legal requirements and standards for cyber security. For example, the legislation can mandate that companies manufacturing IoT devices or developing AI applications follow certain security protocols and adhere to specific cyber security standards. Such legislation can also incentivize (e.g., through funding schemes) companies to prioritize cyber security in the development of new technologies. In the data privacy domain, we witnessed a successful proactive legislation of the COVIDSafe app with bipartisan support from both the government and opposition parties in 2020. Although, eventually, the app itself did not prove to be effective, lessons can be learned with regards to mobilising support for legislating emerging technologies[55].

- More generally, organisations should promote a data-centric approach to cybersecurity that places a premium on protecting sensitive data. This requires organisations to understand the value of their data and take a risk-based approach to data protection. This includes implementing data classification, access controls, and encryption, as well as data backup and recovery plans.

[55] https://espace.library.uq.edu.au/view/UQ:484bb30

- On this note, organisations must approach data security and cybersecurity with a commitment to ethical principles that respect the rights of individuals and protect their personal information. One key ethical consideration is the principle of data minimisation, which means collecting only the data that is necessary for the stated purpose, and minimising the use of personal data for secondary purposes. Organisations should ensure that they are collecting and using personal data in a lawful, fair, and transparent manner, and that individuals have control over their personal data.

20. How should government measure its impact in uplifting national cyber resilience?

- Cyber resilience is a complex concept that stems from measures and actions taken to strengthen preparedness and prevention for, as well as response to, and recovery from, cyber-breaches. Traditionally, emphasis has been placed on the first two stages. The acknowledgement that, despite best efforts, total security from cyber-breaches is virtually impossible, has led analysts and practitioners to underline the importance for countries (and organisations) to increase their investments in response and recovery. Measuring the impact of initiatives aimed at uplifting national cyber resilience requires therefore the development of adequate processes and metrics across the four aforementioned stages. This is particularly relevant considering that, to date, there is no agreed-upon mechanism to measure cyber resilience.

- At the same time, establishing appropriate metrics for cyber resilience cannot be done without consideration for the types of adopted metrics: these should be carefully crafted to balance input and output indicators, with varying degrees depending on the four stages. For example, utilising the number of incidents occurred in the country in a set timeframe would only offer a very limited perspective on Australia's overall cyber resilience. A more complete overview could be achieved by including input indicators, such as, for example, budget allocations towards initiatives for cyber resilience, size and diversity of the cyber security workforce in the country, number of organisations certified against international standards, etc.

- On another note, environmental indicators should also be considered, in order to offer an understanding of the country's susceptibility to cyber-attacks (e.g., attack surface). A proxy that can be utilised to do so is the degree of 'cleanliness' of the cyber ecosystem. For example, having several servers in an environment that allows NTP mode 7 response is a condition conducive of possible Distributed Denial of Service attacks (DDOS)[56]. The Strategy should incorporate measures on how the government could act as a platform for the monitoring of the degree of 'cleanliness' in the country, in the framework of a comprehensive mechanism to measure the country's cyber resilience.

- The establishment of strong collaborative ties between industry, government, and academia/research in this field is a *conditio sine qua non* for Australia's effective monitoring and management of cyber resilience. On this note, exemplar initiatives exist around the world, which could be used as a source of inspiration[57]. Once more, involving relevant stakeholders and connecting them through a safe space conducive to meaningful information sharing (e.g., indicators, statistics, 'push' and 'pull' data collection

[56] https://supportportal.juniper.net/s/article/Updated-NTP-Mode-7-Denial-of-Service-Vulnerability-VU-568372?language=en_US
[57] https://cybergreen.net/

models, etc.) is of utmost importance. At the same time, involving the general public in meaningful conversations on, and genuine engagement with, cyber security and privacy, is key to the enhancement of the national cyber resilience.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

- As mentioned at the beginning of this submission, a strategic document that does not indicate clear goals and objectives, and instruments to monitor and measure their achievement, is incomplete. The Strategy, in this sense, should be a technical document created with the purpose of setting the stage, establishing the goals, and identifying performance measurement and management methods.

- As a result, evaluations to foster transparency around the Strategy and sustained inputs to its design and re-design should include the following design criteria:
    - The Strategy as a 'living document' (e.g., on a publicly available website) subject to change, not drafted once for good;
    - Key Performance Indicators (KPIs) established based on the critical features of being Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART)[58];
    - An ongoing monitoring and management mechanism, potentially involving an independent, governmental entity;
    - Regular review processes, aimed at moulding the Strategy based on the ever-changing threat landscape, to keep the document up to speed with technological developments and emerging adversarial behaviours;
    - Public *fora* for wide-spread feedback on the relevance and performance of the Strategy (on the model of the present call for submissions on the DP).

- It will also be important to consider and acknowledge the different institutional logics that will come into play during the Strategy execution, beyond the mere establishment of a few metrics and KPIs. Institutional logics are the "socially constructed, historical patterns of cultural symbols and material practices, assumptions, values, and beliefs by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their daily activity"[59]. As an example, the institutional logic applied by a multi-organisation critical infrastructure in its contribution to pursuing the goals established by the Strategy may drastically differ from the one adopted by a government agency. Recent research has identified the following practical steps that complement the more technical aspects of strategic planning and evaluation[60]:
    - Taking time to understand and engage with the logic underlying the behaviours of stakeholders involved in evaluations;
    - Identifying ways to unpack institutional complexity and institutional logics without being naïve about the difficulties involved in politically-sensitive contexts;

[58] https://www.business.qld.gov.au/running-business/planning/goals-kpi
[59] Reay, T., & Jones, C. (2016). Qualitatively capturing institutional logics. *Strategic Organization*, 14(4), 441-454.
[60] Burton-Jones, A., Akhlaghpour, S., Ayre, S., Barde, P., Staib, A., & Sullivan, C. (2020). Changing the conversation on evaluating digital transformation in healthcare: Insights from an institutional analysis. *Information and Organization*, 30(1), 100255.

- Engaging in targeted evaluations for specific purposes (e.g., different approaches to measurement for different logics), rather than one evaluation for all needs;
- Employing various communication styles about the results of the evaluations, depending on the audience and the logics they ascribe to.

Contributors' List (Alphabetical Order)

Sasenka Abeysooriya, Senior Strategic Adviser – UQ Information Technology Services

Saeed Akhlaghpour, Senior Lecturer in Information Systems - UQ Business School and UQ Cyber

Ivano Bongiovanni, Lecturer in Information Security Governance, Policy, and Leadership - UQ Business School and UQ Cyber

Dallas Dowsett, Head of International Development – UQ Global Partnerships

Joseph Grotowski, Head of School – UQ School of Mathematics and Physics

Mike Holm, Senior Manager – AusCERT

Dan Kim, Associate Professor in Cyber Security – UQ ITEE and UQ Cyber

Ryan Ko, Professor, Chair of Cyber Security and Director of UQ Cyber

Andelka M. Phillips, Senior Lecturer in Law, Science, and Technology – UQ TC Beirne School of Law and UQ Cyber

Sergeja Slapnicar, Associate Professor in Accounting – UQ Business School and UQ Cyber

David Stockdale, Director of Cyber Security – UQ Information Technology Services

John Swinson, Professor – UQ TC Beirne School of Law and UQ Cyber

Geoffroy Thonon, Senior Analyst – AusCERT

Mark Utting, Associate Professor in Software Engineering, UQ ITEE and UQ Cyber

Brendan Walker-Munro, Senior Research Fellow, UQ TC Beirne School of Law and UQ Cyber

Shannon Willoughby, Executive Director - UQ Government Partnerships and Policy