macquarie
TELECOM GROUP

Submission to the

Australian Cyber Security Strategy 2023-2030 Discussion Paper

14 April 2023

PUBLIC SUBMISSION

Introduction

1.1 Macquarie Telecom Group Ltd (**Macquarie**) welcomes this opportunity to contribute to the Department of Home Affairs Discussion Paper on the Australian Cyber Security Strategy 2023-2030 ('**the Paper**').

1.2 Macquarie supports the goal articulated in the Paper, for Australia to become the most cyber secure nation in the world by 2030, and we acknowledge the ambition of this goal, given Australia's current cyber security position globally (e.g. Australia is ranked 12th in the Global Cybersecurity Index).

1.3 We agree with the statements from the Paper – achieving this goal by 2030 will require "an integrated whole-of-nation endeavour" comprising a "coordinated and concerted effort by governments, individuals, and businesses of all sizes." We believe achieving this goal will not be possible without significant Government funding, significant regulatory change, and cross-government prioritisation.

1.4 Macquarie's interest in the Australian Cyber Security Strategy 2023-30 touches many areas highlighted in the Paper and we have done our best to respond to each question therein. Our submission is focused on the Government's goal for Australia to be the most cyber secure nation in the world by 2030 and, where possible, we have detailed practical solutions we believe are critical to achieving this goal.

1.5 Macquarie is subject to the Security of Critical Infrastructure (**SOCI**) regulatory regime in multiple capacities: as a licensed carrier under the *Telecommunications Act 1997* (Cth), a cloud service provider, and the owner and operator of Australian data centres that store and process the data of Commonwealth and State/Territory governments, as well as critical infrastructure providers and corporate customers.

1.6 Macquarie's data centres and cloud services are "certified strategic" under the Commonwealth Government's Hosting Certification Framework (**HCF**). Macquarie is the only company to achieve certification under the HCF for both data centre and cloud services.

1.7 Through secure internet gateway services, cyber security and secure operations services, Macquarie provides cyber security and secure data storage/processing to approximately 42% of the Commonwealth government, measured by headcount.

1.8 For many years Macquarie has been investing in and advocating for the goal for Australia to be a leading cyber secure nation. The strategic decision to locate and construct our data centres in Australia and achieve HCF certification are clear evidence of our ongoing and longstanding commitment to supporting a robust cyber security posture for Australia.

1.9 We also wish to acknowledge that cyber security cannot be considered in isolation. We recognise the importance of other key Government reforms, including the review of the Privacy Act, the Digital Platforms Review and the implementation of the Consumer Data Rights as key.

1.10 In sum, Macquarie is an important stakeholder in the development of the Australian Cyber Security Strategy 2023-30 and we hope the Department of Home Affairs finds our input both insightful and useful.

General observations

Q1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

A unified approach across government, the private sector and the wider economy

1.11 As the Paper makes clear, for the Australian Cyber Security Strategy 2023-30 (**the Strategy**) to be a success, a true "Team Australia" approach is needed. The legislative landscape applicable to cyber security and privacy has evolved overtime and is currently ad hoc and fragmented across Commonwealth and State/Territory levels, as well as industry-specific frameworks.

1.12 Therefore, the Strategy must establish cyber security as a unifying nationwide endeavour, led by the Australian Government as exemplar, but delivered throughout all tiers of government, the private sector and the wider economy.

1.13 We submit, that to achieve the goal of being the most secure nation by 2030, each of these stakeholders must be 'uplifted' and enabled to collaborate. This can only be achieved if a nationwide approach is adopted.

1.14 Therefore, the Strategy needs to be fully elevated within Government to raise its importance across the whole-of-government, and to establish governance over all Government departments and agencies (including Corporate Commonwealth Entities) as well as Australia's second (State/ Territory) and third (Local) tiers of government, and critical infrastructure sectors. This will ensure the Strategy can influence matters above and beyond the remit of the Department of Home Affairs.

1.15 The Prime Minister, along with State Premiers and Territory First Ministers should jointly create and/or own the Strategy, if necessary, co-signing or co-writing the foreword, with the intention of ensuring State and Territory cyber security strategies 'ladder-up' to the national Strategy.

1.16 Similarly, other cyber security strategies already applied at the Commonwealth Government level, must ladder-up to the national Strategy. This is a point Macquarie made in its submission (Appended to this document) to the Defence Strategic Review in relation to the Department of Defence ICT Strategy and Department of Defence Cyber Security Strategy, both released in August 2022:

> *[The Australian Government must consider] aligning, where cyber security is concerned, the recent Defence ICT and Cyber Security Strategies with other related initiatives, including the Defence Sovereign Industrial Capability Assessment Framework (for determining priorities), and the Defence Capability Framework (for building and managing capabilities), under the National Cyber Security Strategy.*

1.17 For the Strategy to succeed, all Departmental cyber plans and strategies, along with all State/Territory and local government strategies, must be subordinate to the national Strategy. Responsibility and accountability should be explicit but shared.

1.18 We acknowledge the difficulty that will likely be faced making State-based and local government strategies subordinate to the national Strategy, notwithstanding the current fragmented regulatory landscape. For example, currently State/Territory and local Governments are regulated by a range of state-based privacy and surveillance laws together with variation in cybersecurity maturity across the various levels of State/Territory and local governments.

1.19 Additionally, to achieve the Strategy's goal, it is vital that the Strategy uplifts all organisations, with particular effort required by small and medium-size enterprise (**SME**). A significant number of SMEs have an immature understanding of cyber and privacy risks. A potential driver for this is the Privacy Act which has an exemption for small business, which means that many SME have not had to comply with privacy or basic security obligations. Given the vulnerable position of many SME, the Australian government will likely need to provide these organisations with targeted additional support.

1.20 In summary, to achieve the goal of being the most cyber secure nation by 2030, the Strategy must be focused on uplifting everyone, not only the entities subject to SOCI. This will have the added effect of uplifting the cybersecurity awareness and literacy of Australian citizens.

Longer-term strategy goals

1.21 We consider that the Strategy's timeline of 2023 – 2030 (7 years) is relatively short, and that it may be ambitious to achieve the goal of being the most cyber secure nation in this timeframe given Australia's current standing. It may be helpful to include secondary, longer-term plans and goals within the Strategy or, at a minimum, articulate that the goal extends beyond 2030 with a clear intention to periodically review the Strategy's progress.

Clarity on the Strategy's goal to make Australia the most cyber secure nation by 2030

1.22 To ensure that the Strategy's goal is meaningful, we recommend the Strategy clearly set out what it defines as the "most cyber secure nation", which nation(s) currently holds that title, and the metrics through which the title is measured. This will allow Australia to benchmark its progress towards that goal by 2030.

1.23 The Australian government may wish to use the Global Cybersecurity Index as an objective metric, as this Index measures countries' cybersecurity commitment in the following five key areas: (a) legal measures; (b) technical measures; (c) organisational measures; (d) capacity

building measures; and (d) cooperative measures, and ranks countries by their commitments. In the Global Cybersecurity Index, Australia is currently ranked 12th and the USA is ranked 1st.

1.24 We submit that our practical submissions to the Paper are firmly aimed at progressing Australia's ranking towards the goal of being the most secure nation by 2030.

Promotion of independent decision-making

1.25 The Strategy should also be designed to promote and enable independent strategic decision-making by Ministers, the bureaucracy, and corporates, rather than just providing cover for a laundry list of specific reforms.

1.26 To this end, to reflect the different audiences who will use the Strategy, it should comprise two parts or versions – one confidential and one public. The confidential version should be releasable to Commonwealth and State/ Territory and local governments, should candidly explain the threat environment, and set out principles or decision criteria to guide strategic decision making by the bureaucracy (e.g., contracting, procurements, policy making, budgeting).

1.27 This should have the effect of providing a basis for departments and State/ Territory and local government to assess whether their cyber security decisions are consistent with the national Strategy and with the need to secure the whole-of-Australia.

Flexibility to accommodate the rapidly changing cyber landscape

1.28 A real issue is how the pace of technology change and the pace of cybersecurity threats far outstrips the pace of legal reform. Australia's fragmented legislative landscape underscores and exacerbates this challenge.

1.29 To be successful, the Strategy must be flexible enough to respond to the rapidly changing cyber landscape and should be able to accommodate entirely new types of data, ways of handling data, and cyber threat behaviour which may develop within the next decade.

1.30 To this end, the Strategy must focus more on outcomes and less on inputs (funding new programs to uplift cyber, for instance). Cyber security is a highly dynamic environment where cyber criminals and state actors are constantly making moves and countermoves to inflict harm upon us. We should expect this to continue long after the Strategy has been released and put into effect.

1.31 Greater inputs will not prevent cyberattacks from succeeding but fostering a national culture of strategic decision making (ie. an outcome) will mitigate their impact and help reduce the rate of successful cyberattacks over time as a more preventative national culture change begins to take effect.

Ethical considerations

1.32 We submit that the Strategy should also consider and address ethical concerns relating to technology, in particular, those relating to artificial intelligence (**AI**) systems. AI poses three major areas of ethical concern, being (a) the implementation of mass surveillance and facial recognition technology; (b) bias and discrimination hard-wired into the AI's training, which has already proven to affect human rights and equality of opportunity; and (c) our diminishing control over AI as it becomes increasingly advanced. In short, AI and ethical considerations is likely to be a key cybersecurity concern.

1.33 Accordingly, it is appropriate for the Strategy to consider and address the issue. Regarding AI, the Australian government can refer to frameworks already being developed by other countries, such as The Artificial Intelligence Act proposed by the European Union and Singapore's Model AI Governance Framework.

Commitment to funding for the Strategy

1.34 Given the significant level of funding that will be required to achieve the Strategy's goal of being the most secure nation by 2030, the Strategy should indicate the Government's funding commitments towards achieving this goal.

1.35 We consider that including clear funding commitments will lend legitimacy to the Strategy and its ambitious goal and will foster industry and broader stakeholder support.

1.36 For reference and acknowledging population and other geopolitical differences, the USA (designated the "most cyber secure nation in the world" by the 2020 Global Cybersecurity Index, and in 2021) allocated $18.1 billion in cybersecurity funding to protect government systems and citizens.

Legislative and regulatory reform

Q2. 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)?*
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?*
c. *Should the obligations of company directors specifically address cyber security risks and consequences?*
d. *Should Australia consider a Cyber Security Act, and what should this include?*
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?*
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?
(i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?
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?*

(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)?

2.0 We believe the Australian Government is adopting the right balance with respect to the mix of legislative and regulatory regimes to uplift Australia's cyber security.

2.1 However, to implement a national Strategy, there are challenges given the fragmented nature of state-based privacy and surveillance laws governing State/ Territory and local Government.

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

2.2 In 2023 cybersecurity is now a major risk which must be managed by Boards and directors across Australia. We believe that company directors would benefit from principles-based guidance, setting out what a reasonable company director (of different types of companies) need to be doing to adequately manage cyber risk. We acknowledge ASIC has released a body of guidance aimed at directors and Boards to address this. We also acknowledge that on 5 May 2022, ASIC was successful in the Federal Court after the Federal Court made declarations that RI Advice Group Pty Ltd (**RI Advice**) breached its obligations under: s 912A(1)(a) of the Corporations Act 2001 (Cth) Act by failing to ensure adequate cybersecurity measures were in place and/or adequately implemented across its Authorised Representatives (AR); and s 912A(1)(h) of the Corporations Act 2001 (Cth) Act by failing to implement adequate cybersecurity and cyber resilience measures and exposing its ARs' clients to an unacceptable level of risk.

2.3 The ASIC v RI Advice establishes that the content of general obligations under s 912A of the Corporations Act 2001 (Cth) Act for AFSL holders extends to a consideration of cybersecurity matters.

2.4 The ASIC v RI Advice case has limited application (i.e., it is restricted to entities which hold an AFSL). In addition, the case provides limited practical guidance on what Boards and directors should be doing to address cyber security risks.

2.5 Macquarie submits that given the ASIC v RI Advice case, there is an opportunity to consider in more detail the obligations of company directors specifically to address cyber security risks and the consequences in the longer term.

2.6 However, in the meantime and during this settling period, the focus should be on uplifting the cybersecurity maturity of Boards and directors in Australia through other measures outlined in these submissions. Many Boards and directors remain ill-equipped to manage the evolving cybersecurity threat environment and are ill-prepared to respond to a major incident.

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

2.7 During the settling period, there is other work Government can do that would help prepare the machinery of government for the introduction of further reform, which may include a Cyber Security Act.

2.8 Since cyber security is a 'horizontal' responsibility that cuts across the whole of government, notwithstanding the many ministerial, legislative and departmental responsibilities which involve cyber in some way(s), there is a case for reforms that will enable clearer and more efficient cooperation at the inter and intra-department level, and across ministerial offices that share responsibility for cyber, data protection and privacy policy regimes and regulations.

2.9 An internal review and allocation of ministerial and departmental roles and responsibilities to respond to future serious cyberattacks (ie. either against Government or private sector entities) should be undertaken, with recommendations from that review also given time to take effect—we suggest during the same SOCI settling period that industry will go through from 17 July 2023.

2.10 Such a review would be a worthwhile exercise in preparation for a Cyber Security Act, since one effect of any new regime should be 'knitting together' the multiple existing regimes where cyber security is concerned.

2.11 Such a regime will need to be supported by multiple stakeholder ministries—hence the recommendation for internal review to precede creation of a Cyber Security Act.

2.12 We also recommend the Australian government use this preparation time to evaluate existing cyber security laws and frameworks globally and learn from approaches other countries are taking. For example, the frameworks established by Singapore's Cyber Security Act and the EU's Cybersecurity Act may provide useful reference materials to guide and assist the approach Australia might take.

2.13 Adopting this cadence will ensure a new Cyber Security Act provides new clarity both government and the wider economy as to how existing regimes interlink/ interact and have the effect of clarifying the roles and responsibilities multiple stakeholder ministers and their respective departments will have for administering the related cyber security regimes.

2.14 Government entities deal in very different types of information to commercially run critical infrastructure operators. However, the security, integrity and accessibility of that government data is no less critical to the continuous functioning of society. Commonwealth and State/ Territory data needs to be brought back into the protective regulatory regime for Australia's critical infrastructure, noting that, given the pace of technology change, the types of data handled by government in 2030 may include wholly new types of data that we cannot currently predict.

2.15 We believe the Australian Government should also be looking to introduce a data classification scheme for government data which harmonizes with the States/ Territories and is extendable to commercial critical infrastructure providers. We understand the Department of Home Affairs was considering such an initiative as part of its development of a Data Security Action Plan.

2.16 More immediately, we suggest the Minister for Home Affairs and Cyber Security be given a statutory power to declare a particular type of data, or a particular data workload, to be of national significance and thereby prevent it from being stored or processed outside of Australia if such an outcome would not be in the national interest.

2.17 As set out above, this kind of flexibility is required due to technology's fast pace of change, which may involve new types of data being introduced that are not yet envisaged. By way of example, this might be appropriate for:

- the clearing and settlement systems and central securities depositories that underpin the operations of the Australian Securities Exchange;
- the inventory or logistics management systems used by private sector participants involved in the management of Defence assets, the National Medical Stockpile or similar national resources;
- automated remote patient monitoring platforms used in public hospitals; or
- certain non-active data sets, such as the blueprints or schematics of key institutions (e.g., Parliament House) or infrastructure (e.g., the East Coast gas grid) or bathymetry survey data (ie. the topography) of the Australian sea floor.

2.18 Such a Ministerial power would align with the Treasurer's existing power and recent practice under the *Foreign Acquisitions and Takeovers Act 1975* (Cth) to impose data conditions on foreign takeovers.[i] Ironically, as things stand today, a company can be prevented from shifting critical data offshore if a foreign investor acquires a controlling stake in the business but not if the business remains Australian owned.

(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?

2.19 Macquarie's position is that the Strategy requires a 'Team Australia' approach for all stakeholders to be uplifted. We consider it important for the Strategy to account for and monitor the regulatory burden in relation to legal obligations relating to cybersecurity. As noted in this submission, we consider the compliance burden on some entities, such as SME will be significant, compared with other entities and stakeholders who have a more mature cybersecurity posture.

2.20 Broadly speaking, we favour national strategic oversight over streamlining existing regulatory frameworks. However, we would caution that some entities—SMES for instance—will likely struggle with additional compliance burdens,

(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?

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

2.21 Macquarie acknowledges the complexity of this topic and the Government's current position that ransom demands should not be paid. However, a strict prohibition on the payment of ransom demands could have unintended consequences. For example, a prohibition on the payment of ransoms may not deter organisations from paying where to not do so will prevent the organisation from continuing to run its business.

2.22 Legislating against the payment of ransoms may even further reduce the likelihood of voluntary disclosures on cyber incidents to government agencies and may simply have the effect of driving cyber incident response further underground with no governmental oversight and support. This may impede the Strategy's goal from being achieved.

2.23 Furthermore, criminalising the payment of ransoms arguably punishes the organisation, which is already the victim of a cybercrime, whilst only indirectly punishing the threat actor. Instead, we consider that the government's resources would be better utilised in supporting such organisations to mitigate the damage, rebuild and prevent further incidents.

2.24 The impact of a strict prohibition on the payment of ransoms may result in actual harm to individuals as there may be circumstances where lives are threatened. For example, a threat actor may lock-down mission critical security systems to lock individuals inside a secure building posing risk of injury or death to the individual inside the building.

(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?

2.25 We believe the Government's position on the non-payment of ransoms is clear. The Australian Cyber Security Centre (**ACSC**)'s guidance to not pay a ransom has been widely communicated by the media, and the rationale for non-payment is clearly and concisely set out on the ACSC's website. However, the topic is nuanced and there is an opportunity to provide more guidance on the issue.

International context

Q5. 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?

5.0 For Australia to reach the Strategy's goal by 2030, it is imperative Australia, at a minimum participate in and further, where possible, aim for a leadership role in existing forums and cybersecurity thought leadership processes within the region and internationally. These include the ASEAN Ministerial Conference on Cybersecurity, the Global Conference on Cyber Capacity Building and the Cyber Security Asia Conference.

5.1 Where there is a gap in international standards-setting, Australia may consider establishing a forum which we would host to address that particular gap in order to better contribute.

5.2 We note that the ACCC is currently undertaking the Digital Platforms Review which is being watched globally, with other regulators appearing more willing to take enforcement action following the lead of the ACCC.

5.3 Likewise, the Australian Government has taken a leadership position in the fight against the complex global problem of modern slavery by publishing a 'world first' Government run register for modern slavery statements. Other jurisdictions are now looking to Australia's modern slavery Act and reporting requirements as a leading example.

5.4 We consider there to be similar opportunities for the Australian Government to take a leadership position when it comes to cybersecurity.

Government cyber leadership

Q7. What can government do to improve information sharing with industry on cyber threats?

7.0 Macquarie believes the sharing of threat intelligence information is critical. Given that the current threat landscape is evolving rapidly, as are the types of threats, it is important that information about cyber-attacks is shared quickly, to educate the community on the types of threats being posed. Disseminating this information quickly through use of electronic threat reports is an option worthy of exploration.

7.1 We believe Government has an under-utilised asset in the Joint Cyber Security Centres (**JCSC**), which could be further funded to support threat intelligence sharing with industry.

7.2 The idea behind the creation of the JCSCs, to give the Australian Cyber Security Centre presence in each State and Territory, in the interests of leading cyber security uplift nationally, was a welcome and much needed initiative. We believe the Strategy provides significant opportunity to expand the remit of the JCSCs and utilise them to help deliver the Strategy's goal.

7.3 To begin with, we suggest each JCSC be funded to organise around specific industry clusters present in each State/ Territory, focusing their intelligence efforts accordingly.

7.4 In practical terms this would mean funding the JCSC in Perth to include a subject matter expert (SME) with cyber expertise relevant to the resources and mining sector; the JCSC in Adelaide would include a SME with cyber expertise relevant to defence industry; similarly banking and finance in Sydney and Melbourne. Where multiple sectors cluster in certain market—technology/ ICT and banking/ finance in Sydney for example—multiple SMEs would be funded where appropriate. Armed with this expertise, each JCSC would be well placed to tailor their intelligence sharing and information guidelines to their respective markets.

7.5 In terms of intelligence sharing with industry, we recommend the ACSC develop a 'trusted network' of organisations which should include private companies which are actually monitoring cyber security threats at scale. The trusted network would act as an aggregator of cyber intelligence data and work closely with ASD/ ACSC to turn their collective data into unclassified briefs which Government and the trusted network would share with wider industry sectors. The intent is for Government to leverage Australia's existing cyber industry capabilities which are already being applied and direct them to help affect cyber uplift across the economy. This would

7.6 Naturally, ASD/ ACSC should arbiter pre-requisites for qualification to the trusted network. We would anticipate these to include requisite security cleared staff, as well as both data volume and quality/ format standards.

7.7 The JCSCs could also deliver initiatives targeting cultural change across industry clusters in each State/ Territory in the form of Board and C-level presentations to industry stakeholders, providing them cyber security briefings bespoke to specific sectors. This approach would compliment the current Cyber Threat Intelligence (CTIS) program being run by the ACSC, which is achieving some success targeting CIO/ CISO level leaders in industry. Further engagement could be delivered through the JCSCs in the form of online/ electronic communications to their respective members/ stakeholders.

7.8 Additionally, we recommend that the Strategy prioritise innovation such as implementing technological solutions using data analytics that enables the rapid analysis of threat trends and report information to support data breach response. Innovative solutions could potentially also provide organisations with practical recommendations on response activities, which may be of particular benefit to SMEs with fewer resources and less experience in handling security incidents.

Q8. 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?

8.0 Where intelligence sharing is concerned, the challenge for regulators is balancing the benefits sharing provides organisations at risk of cyberattack (ie. potentially every organisation connected to the Internet) with the risk of potential regulatory or enforcement action, or reputational damage to the individual organisation that is the victim of cyberattack.

8.1 As a provider of cyber security services to many private and public organisations, we would argue the overall benefit to cyber security incident management and shared learning potentially outweighs the risk.

8.2 Of course, our risk analysis is focused on the wider economy—the cyber security risk—more than individual company reputational risk. Our perspective will likely not be shared by an individual company successfully targeted by cyberattack.

8.3 Nevertheless, an explicit obligation of confidentiality with the ASD/ACSC would promote voluntary disclosures, which would be of substantial benefit to the Australian community in permitting intelligence sharing at widest possible scale, and helping organisations across Australia learn about and protect themselves against specific types of cyberattack. In this regard there is scope for the ASD/ACSC to create their own disclosure requirements, which would not contradict this were it in place.

8.4 Rather than reinvent the wheel, the ACSC should be reusing what has already proved successful for tracking criminal activity. A good example is the Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF), with mandatory reporting (with confidentiality assurances) through a single portal.

8.5 In addition, the Consumer Data Right (CDR) legislation is founded on the idea that consumers own their data and should therefore control it. CDR has been rolled out to lenders already, and it is legislated to be rolled out across the entire economy.

Q9. 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?

9.0 In short – yes, it would. Without a mandatory reporting regime Australia cannot determine the nature and scale of cyber security threats being made against us. This is problematic in determining the best strategy for addressing the threat environment which is often more significant than many realise.

9.1 However, we would anticipate significant pushback from the private sector on this idea, and it would only be effective if supported by robust, clear information dispersal to the public—a form of reporting framework respected by everyone who reports it (ie. the media). We also note that expanding this regime would cause it to be inconsistent from the mandatory data breach regime under the Privacy Act, which requires notification only for incidents involving personal information.

9.2 Where the Strategy expands the cyber incident notification regime, care should be taken to still include a seriousness threshold, so that the notification portal is not overwhelmed from receiving reports of minor cyber incidents.

9.3 Similarly, organisations reporting cyber attacks against them must be given peace of mind that their disclosure will not automatically result in public notification, much less public shaming. Mandatory disclosure to the ASD/ACSC is an important tool in our national arsenal against cyber attackers. Our goal should be to create an environment where organisations feel it is safe for them to disclose.

9.4 Furthermore, Australia is currently facing significant 'noise' from media reportage of cyberattacks (notwithstanding recent notable and high-profile incidents), which focuses public discourse on potential damages, and seeks to attribute culpability and accountability. We would argue this type of reportage is not always in the public interest, and can impede efficient data breach response and remediation, as a considerable amount of effort is spent by the affected organisation on managing public reputation.

9.5 If public cyber discourse centred around 'shock and awe' media headlines that focus on the number of individuals impacted, we face a risk of 'security fatigue' which may lead to public

apathy whereby people simply give up and accept their networks and data are trivially defended.

9.6 Similarly, Australia must not get into a cycle whereby our media becomes interested only in cyberattacks that impact ever increasing numbers of individuals. The types of data stolen and the harm that cyber-attacks perpetrate on individuals should be of greater concern than the number of individuals affected.

9.7 In this respect, theft of data—home addresses for instance—relating to 100 Australians in witness protection has the potential to inflict much greater harm than theft of similar data relating to 10,000,000 Australians. Similarly, the theft of medical records of one individual—the Prime Minister for example—has the potential to be a national security risk. The number of people affected by data theft should not be the sole determining factor of risk assessment in our public discourse.

9.8 Media and other public communication of cyberattacks would be best utilised focusing public attention towards any new dangers which may be perpetrated against Australians whose data has been stolen and provide practical advice to mitigate those dangers. There is an opportunity to potentially change the media discourse with the proposed Privacy Act reforms, which in part align with GDPR obligations. However, the government will need to focus on public education to influence the media to change its discourse from a focus on numbers, to a focus on harm and on sharing practical solutions to prevent cyber-attacks.

9.9 The EU has made cybersecurity a relevant topic to the general public at a much greater scale with education on the GDPR, and cyber security remains a topic of public discourse which does not requires cyber-attacks to impact increasing numbers of people to remain relevant.

Q10. What best practice models are available for automated threat-blocking at scale?

10.0 Our response to this question comes from our technical team, and subsequently refers to specific capabilities. We will be happy to offer our technical experts to the Department should additional clarification be sought in relation to this specific item.

10.1 Our views on automated threat blocking come from learned experience from which we know that it is not enough for security software tools to do actual configuration changes on an ongoing basis. Processes also need to be augmented to keep up with technology changes.

10.2 A threat intelligence platform (eg. MISP) that is integrated with a SOAR tool that is further integrated with multiple security tools (ie. Firewalls, Proxys, Email Security) in order to be able to automatically block confirmed and high confidence indicators of compromise and threats is an ideal solution for automated high volume threat blocking.

10.3 This solution is optimal so long as the threat intelligence feed is of high quality and high confidence of accuracy. For example, the CTIS feed provided by ACSC would be of necessary quality. From there, the solution can be automated with both open source free and premium vendor SOAR tools to automate threat blocking that is applicable to all.

10.4 This solution can be applied in a way which will free up time of SOC analysts to focus on other higher level bespoke work.

10.5 To enable this solution at scale it is necessary to have the appropriate "pre-approved" integration workflows created and setup in the SOAR platform and a pre-approved change management ticket workflow setup with the agencies chosen ITSM platform (eg. ServiceNow).

10.6 Such a pre-approved "change type" also needs to have a Security Risk Assessment completed by the GRC team to ensure that any automated changes have been assessed appropriately and that all risks have been accepted for this to happen automatically for as long as the solution is engaged.

Q11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

11.0 Macquarie believes Australia does require a tailored approach to uplifting cyber skills. The Strategy cannot merely focus on implementing technology and infrastructure, a significant focus must be on attracting and retaining a skilled workforce to uplift the Australian cyber security regime to achieve the Strategy's goal.

11.1 In its 2022 Sector Competitiveness Plan, AustCyber reported that Australia will fall well short of its required cyber security workforce by 2026:

> *"Australia's cyber security sector is expected to have 3,000 fewer workers than required by 2026, despite projected growth of 1,200 workers over the period. Demand for cyber security workers will increase to 51,100 workers by 2026. However, based on projected inflows and outflows from the cyber security workforce, by 2026 there will be a shortage of 3,000 workers. Only 48,100 of the demanded roles will be filled."*[1]

11.2 These findings suggest the Government's broader STEM agenda is proving insufficient in providing the requisite cyber talent pipeline required in Australia. As a major cyber security employer, reliant on security cleared engineers whom we employ to support the protection of government data, Macquarie is highly sensitive to market trends where skills and talent are concerned.

11.3 We, like our customers, partners and competitors, operate in the technology sector which has been experiencing unprecedented high demand for talent in recent years. The shortage of available talent has not been helped by predatory recruitment tactics by global corporations which have inflated salaries far in excess of the consumer price index.

11.4 Macquarie believes Australia will benefit from Government playing a greater role to develop a cyber security talent pipeline, in particular utilising underleveraged assets to help deliver this need.

11.5 Cyber security benefits from skills acquired across a spectrum of levels, with Computer Science and related university degrees, sitting at the higher end of the spectrum. A gap exists at the lower/ entry level, providing industry can agree on professional accreditation standards that make graduates job ready for the sector.

11.6 TAFE is the ideal institution for such courses. We recommend Government fund TAFE to rollout cyber security courses at scale to grow Australia's cyber talent pipeline. Baseline TAFE qualifications should get graduates job ready for roles in Secure Operations Centres in businesses such as (and including) ours which provide cyber security services to multiple organisations, as well as in-house cyber security positions in the public and private sectors.

11.7 Government should also fund marketing and communications activity to promote interest in TAFE Cyber Security training courses.

11.8 In terms of course development, we understand Government has recently launched its Jobs and Skills Councils in order to:

> *"…identify skills and workforce needs for their sectors, map career pathways across education sectors, develop contemporary VET training products, support collaboration between industry and training providers to improve training and assessment practice and act as a source of intelligence on issues affecting their industries."*[2]

11.9 The Digital Jobs and Skills Council (**DJSC**) will have responsibility for cyber security skills and will include representatives of industry to advise Government and training providers on course standards and content, career pathways, etc.

11.10 We applaud this initiative but recommend Government do more to accelerate it, including better promotion and engagement with industry to ensure its' success. Through the DJSC there is risk course development gets slowed down through industry/ stakeholder engagement. To expedite this, Government has another underleveraged asset it can use to baseline what TAFE cyber security training courses might look like.

11.11 The Joint Basic Cyber Course, run by the Australian Defence Force, is a 9-month program covering vulnerability assessment, incident management, and basic hunting skills. It is ideal as a micro-credential for TAFE and could sit alongside existing university degrees to enable rapid upskilling and grow Australia's cyber talent pipeline.

11.12 Rather than commence course development 'from scratch' through the DJSC, we recommend the Joint Basic Cyber Course be held up as a starting framework for discussion.

11.13 Whilst there is clearly a need for expending our training opportunities, there is also a need for cultural change across the economy. To this end, Government has opportunity to institute cyber awareness training in schools as a way to instil safer online behaviours by school-aged children which might then be carried into adulthood. We note that as schools are operated by

[1] See https://www.austcyber.com/resources/scp-2022/chapter-2
[2] See Industry Engagement Reforms - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au)

State/Territory governments, this will involve the Commonwealth and State/ Territory governments working collaboratively.

11.14 We also recommend opening communication lines with countries whose cyber security is more advanced than Australia's (i.e. by reference to the Global Cybersecurity Index), as they may be able to provide helpful guidance to Australia on how to attract and retain a skilled workforce.

Q12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

12.0 Since paragraphs 11.0 – 11.14 concern education and accreditation initiatives, our response to Q12 will focus on immigration.

12.01 The ACT Government has completed informative research into cyber skills through its Canberra Cyber Hub initiative, which Macquarie is supporting through our involvement on the steering committee.

12.02 That research found close skills alignment between cyber and other vocations where numerical and other pattern recognition are commonly required (accounting, for instance), as well as roles which require a strong governance and security mindset. This has led the ACT Government to consider offering residency visas to migrants who are interested in re-training into cyber.

12.03 This idea interests us despite the fact our cyber security workforce requires Australian security clearances, a point we will return to shortly. Any initiative which grows the non-citizen workforce in cyber, creates opportunity for Australian citizens who may be working in roles that do not require security clearance to transfer into roles which do. Such an idea will increase the overall number of trained cyber security professionals to the benefit of the overall sector.

12.04 Government should consider the re-skilling option as a way to fast-track residency visa applications and grow the talent pipeline. The finding from Canberra Cyber Hub that accounting skills correlate with cyber skills might also be of interest to Government if there is a cohort of accounting skilled migrants seeking residency visas at the national level. Accounting is a diminishing vocation due to advances in AI solutions, unlike cyber where demand for human resources is only growing.

12.05 In terms of security clearances, industry experience with the Australian Government Security Vetting Agency (**AGSVA**) has been mixed as the agency always seemed to lack the resources it needed to meet demand with clearances often taking in excess of six months to process.

12.06 For businesses such as ours which provide cyber security services to government, scaling up to meet our customers' demands is often challenging as surge workforces must be security cleared.

12.07 We are cautiously optimistic the announcement on 30 March to move responsibility for Top-Secret level security clearances over to the Australian Intelligence and Security Organisation (**ASIO**) will reduce the processing time for lower-level clearances.

12.08 However, we would caution Government to ensure ASIO gets the necessary resources to meet its new responsibility and, more importantly, there is no cannibalisation of those resources from AGSVA over to ASIO to fulfil its new function. Any change by Government with respect to security clearances should be considered in the context of reducing clearance processing time.

12.09 In this regard, Government might also want to consider implementing a priority ranking system that allows clearance applications of some people in certain circumstances to be 'fast-tracked'.

12.10 There are often instances where government agencies require time-sensitive capabilities to be implemented by individuals who might be on a waiting list for security clearance. In such instances, it makes sense for Government—presumably through AGVSA—to have the authority to move such individuals to the front of the processing queue.

Q13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

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

13.0 In terms of a single reporting portal for entities affected by cyber incidents, we do not believe it is viable to bring all existing reporting portals under a single banner.

13.1 Regarding the form of reporting by organisations subjected to cyberattack, Government could provide stronger guidance and controls as to what is expected of organisations regulated under cyber security regimes. If regulators had more stringent reporting requirements to Government,

and the necessary power to enforce this on regulated entities, those entities could be mandated to produce better quality information and empowered to pursue that mandate.

13.2 Relatedly, Government could consider providing additional funding to ID Care to enable it to provide appropriate support to consumers affected by data theft or other form of cyberattack a hotline for requesting bespoke, specialist advice. A Cyber Ombudsman could then be funded, who would oversee reporting compliance.

Q14. What would an effective post-incident review and consequence management model with industry involve?

14.0 As noted in our response to Q9, there is scope for Australia to 'change the temperature' of cyber reportage and public communications. An effective collaboration between Government, industry and the media require a cultural shift away from 'blame' towards 'learning'.

14.1 Australia should seek to create a safer space for individuals and organisations to disclose without fear of punitive response. Doing this will require Government creating mechanisms that guarantee a degree of confidentiality so that the intelligence relating to each attack, and lessons learnt, can be disseminated throughout the economy and not weaponised for competitive advantage. This will necessarily include a transparent mechanism for how incident learnings are consumed and then used to improve existing standards.

14.2 This may take the form of 'public reports' released after data breaches have occurred, which contain details on how the data breach happened so that others can learn from it. Releasing such reports in conjunction with the government or a regulator could also help to change the narrative. As a case study for this, after ANU suffered a major data breach in 2019, it released a public report as a practical case study, to enable the community to be uplifted and benefit from ANU's learnings.

Q15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

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

15.0 Firstly, we would like to reiterate how important it is that Government ensure cyber security compliance of all organisations and individuals is uplifted to the same level. Given that SMEs are currently not captured by the Privacy Act (and given that SMEs constitute about 95% of Australian businesses), the vast majority of Australian businesses will be starting from a very low level of understanding about cyber security and privacy as it applies to their business, and it will be difficult for these businesses to catch up. Such entities are not required to destroy data in line with Privacy Act requirements, and this is a significant cyber security risk facing Australia currently.

15.1 As suggested in our response to Q13, there is merit in addressing a range of areas relating to victim support. An important issue for victims of cybercrime is the reality that the location—both at rest and in transit—of their data is usually opaque. Organisations which use and collect data are often resistant to data transparency—i.e. how they got data, what permissions were granted, how the data is used, and the countries in which the data is stored and transits through—is a significant exercise for very little commercial advantage. There are also many instances—including among small to medium sized businesses (**SMEs**) where organisations will not want to discard data for fear of losing competitive intelligence.

15.2 A starting point for addressing these challenges would be for Government to implement regulation on how long data sets must be retained. From there, further regulation could be introduced on any new data that is acquired. Such regulations would, over time, gradually 'age out' these issues. Before this occurs, the issue of data location is one which can and should be addressed by Government, focusing initially on government (ie. NCCE, CCE, Federal, State/Territory and local) data, before addressing this risk as it relates to Australia critical infrastructure providers and SONS.

15.3 An easy and practical solution to addressing data theft, would be to require organisations to disclose the location of the theft—in effect disclosing where the data is stored and transits through. This will have the effect of providing the market helpful intelligence when making future decisions on data storage and processing locations.

15.4 Government must take the lead on data location by conducting its own audit of the location of Government data at rest and in transit, and then act on recommendations to address identified risks.

Q16. 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?

Public education

16.0 A key opportunity for the government to enhance Australia's cyber security ecosystem and support uptake of cyber security services is in public education and awareness-raising. Australia's cyber security ecosystem will only be strong if general public users are educated and proactive in identifying and mitigating potential threats.

16.1 Additionally, where consumers are educated in the importance of cyber security, they are more likely to purchase and use cyber security technologies and to see the value in these.

Internet of Things

16.2 "The Internet of Things, or **IoT**, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data."[3] Powered by relatively cheap computer chip production and increasingly ubiquitous Internet connectivity, the IoT presents the next major challenge to policy makers in Australia and around the world.

16.3 In the United States, the US Government (**USG**) has introduced a USG Cyber label for IoT devices to provide enterprises and consumers confidence in the products they are purchasing.

16.4 We suggest the Australian Government seek to adopt this approach, but also ensure Australia's 'Cyber Secure Label' extends to include the supply chain behind manufacture of IoT products, as well as the cyber security capability of those products. This will give Australian consumers confidence not only in the security bonafides of the products they are buying, but also the origin of the full product capability.

16.5 The USG has also recently implemented that country's first Software Bill of Materials (**SBoM**). The website of the US Cybersecurity and Infrastructure Security Agency describes a SBoM as "*a nested inventory, a list of ingredients that make up software components.*" [4]

16.6 The US SBoM is supported by Vulnerability Exploitability Exchange (VEE)—a security advisory that informs product owners in the event a product or products are affected by a known vulnerability/s. The VEE is a practical way of informing people and organisation on masse as/when product vulnerabilities are identified.

16.7 The Government has a number of similar systems currently operating—energy rating stars for consumer electronics, cars and houses for instance—which provide ready frameworks for a new Australian SBoM/VEE to be created.

16.8 The risk of implementing a VEE equivalent advisory or rating system, is that as security issues become more prevalent, that entities may engage in misleading practices and overstate the security capabilities of their products or services. While this may be outside the scope of this submission, regulating such misleading practices may become an enforcement priority for the ACCC in the future, similar to greenwashing.

Q17. How should we approach future proofing for cyber security technologies out to 2030?

17.0 The challenge of future proofing cyber technologies is complex and multi-faceted. It is not just about having the right technology, but it is about educating communities to be cyber risk aware. It is a rapidly evolving and complex landscape.

17.1 One key opportunity for future proofing lies in human resources . A workforce which is technologically aware and possesses solid foundational understanding of IT and cyber, is what Australia needs. This includes staffing Australian organisations with well training cyber professionals who will provide frontline cyber security and drive a culture of cyber awareness.

17.2 Global hyperscale providers license technological capability into Australia, underscoring how our challenge is not to create new technology. Better education at scale is the solution which will provide highest impact at the lowest cost, and deliver manifold impacts across the Australian economy—build a talent pipeline to meet the demands of a growing sector, protect Australian networks and systems from cyberattack, financial and other extortion, et al.

17.3 Macquarie's detailed views on how Government might implement policies to address Australian networks and systems from cyberattack, financial and other extortion, et al.

[3] See https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
[4] See https://www.cisa.gov/sbom

17.4 Building ethical decision-making frameworks, particularly in regards to AI, is critical for future proofing cyber security technologies from causing harm to the individuals they are designed to protect.

17.5 Finally, and as discussed above, we note that from a supply chain and infrastructure perspective, the Strategy should be considering a much longer timeframe than 2030 to have the political impetus to build the major infrastructure required to reach the Strategy's goal.

Q19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

19.0 Macquarie's response to this question is covered in our response to Q16. Specifically, Government should look to the USG's SBoM and VEE as informative, potentially replicable regimes for future-proofing new technologies and promoting security by design. Given the rapid pace of technology change, any policy formation relating to SBoM/ VEE approaches should necessarily be sufficiently flexible to accommodate future and emerging technologies that will connect to the internet.

Measuring success

Q20. How should government measure its impact in uplifting national cyber resilience?

20.0 Macquarie has referenced various measurement tools that are available to track progress toward uplifting cyber resilience across the nation. For easy reference we have summarised these, and included additional suggestions, in the following table:

Measurement metrics	Measured against	Oversight body(s)	Stakeholders
• Increased number of Cyber skilled graduates (TAFE and High Ed) enter the workforce	• Numbers as of 01/2023 • Industry (private and public) demand	• Department of Education • Jobs & Skills Australia	• DJSC • State/Territory and local governments
• Increased number of skilled migrants willing to retrain into cyber	• Numbers as of 01/2023 • Number who enter cyber workforce year-on-year	• Department of Immigration	• Department of Home Affairs • State/Territory and local governments • Business peak bodies
• Reduction in successful Ransomware attacks (measured in dollar value)	• Existing data held by AustCyber, ASIO, et al.	• Cyber & Critical Infrastructure Centre (Department of Home Affairs)	• Department of Home Affairs • State/Territory and local governments
• Increase in corporate reporting of successful cyberattack (ie. Ransomware, DDOS, data theft, et al)	• Existing data held by ACSC/ ASD	• ACSC	• ASD • Department of Home Affairs • Business peak bodies • State/Territory and local governments
• Increase in E8 maturity across Government agencies	• ANAO audit reports; self-reporting by Government agencies	• All Government agencies • ANAO	• Department of Home Affairs

Q21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

21.0 No further commentary.

--ENDS--

[i] *Foreign Acquisitions and Takeovers Act 1975* s 74(2). See also Glenda Korporaal, 'Protect data in foreign takeovers: FIRB chief', *The Australian* (online, 21 August 2019).