TELSTRA GROUP LIMITED

CYBER SECURITY STRATEGY 2023-2030

Discussion Paper

Public Submission

15 April 2023

SUMMARY

Telstra welcomes the opportunity to make a submission in response to the Department of Home Affairs 2023-2030 Australian Cyber Security Strategy Discussion Paper. We support the Government's objectives of uplifting and sustaining cyber resilience and security, and agree that this must be an integrated, whole-of-nation endeavour, that requires a coordinated and concerted effort by Governments, individuals, and businesses of all sizes.

Cyber security is at the forefront of our strategy. It underpins the security of our critical infrastructure and the services we provide to Australian consumers and businesses. We are a strong supporter of industry and Government collaboration and have a long history of working alongside the Australian Government on both operational security and cyber policy issues. While we encourage the Government to be bold in its approach to uplifting cyber security and national resilience, we caution against the introduction of additional regulation, in what is already a complex legislative environment.

Any new regulation needs to be targeted at specific issues and be harmonised with existing regulatory frameworks

Any new regulation should be clear about the problem it is trying to solve. We would welcome additional clarity about the purpose and application of a new Cyber Security Act.

We support harmonising existing data protection regulation and reducing complexity in the storage and protection of data. However, including customer data and systems as critical infrastructure under the *Security of Critical Infrastructure Act 2018* (Cth) (**'SOCI Act'**) is more likely to add to the existing complexity around data storage and protection regulation and is unlikely to result in improved cyber outcomes across the economy.

Raising awareness of cyber risk

We support raising awareness through education and giving boards and business owners the tools they need to make informed decisions around the cyber risks impacting their business. In particular, the Government needs to have a sustained focus in the small business space and engage with larger businesses to help drive innovative thinking around ways to increase awareness about types of cyber risk. This should also extend to identifying opportunities within the education sector to raise the levels of cyber-literacy earlier during a student's schooling life.

Improving the knowledge individuals and businesses have about cyber risks across the economy, and in society, will help them be more prepared to effectively manage and respond to those risks.

Improving Government and Industry Collaboration

Strengthening the collaboration between Government and industry is essential to continue to build and harden Australia's cyber resilience. We support improved threat sharing safeguards, continuing Australia's international role within the Indo-Pacific region and operational initiatives to improve whole of economy cyber preparedness and response.

Threat-sharing collaboration can be improved by strengthening the Cyber Threat Intelligence Sharing (CTIS) platform, via the provision of a human-validated stream of the most important, timely and actionable threat intel indicators.

Operationally, we encourage the establishment of a national cross-sector cyber security exercise and leveraging shared expertise to improve cohesion in response to emerging threats. This would allow Government and industry to establish mutual expectations and thresholds for a nationally significant cyber crisis event.

The Role of Government

The Government has responsibility to be an exemplar of strong cyber security hygiene and best practice. We encourage the Government to commit to a timeline for implementation of Essential Eight for Commonwealth entities. This will provide a clear message that the Government will lead by example.

Further as part of its commitment to evaluation measures in the current Cyber Strategy, the Government should continue using performance metrics for all initiatives developed under the new 2030 Cyber strategy. We also welcome the ongoing publication of implementation progress and suggest considering the value in the dataset collected by 'ReportCyber' being used as a tool to inform evidence-based policy formation.

We strongly support Australia continuing to collaborate with and support countries in our region with respect to cyber resilience. Regional cooperation by engaging with our neighbours is pivotal to understanding the issues that are impacting them to form valuable relationships and meaningful cooperation.

We believe that the creation of a single reporting portal for cyber incidents would simplify reporting processes for entities, where the practical difficulties around different reporting thresholds for cyber incidents and confidentiality restrictions between the Australian Cyber Security Centre (ACSC) and regulators can be overcome. The Government could also consider the creation of an effective post incident review and consequence model, analogous to US' Cyber Safety Review Board (CSRB), with Government and industry representatives.

Uplifting cyber skills

The cyber skills shortage needs to be addressed urgently to plug the immediate gap within the economy and to future proof for the growing rate of the technology sector. We suggest industry, Government, and academia partner to resolve this issue. By way of example, the creation of a central cyber portal that highlights the gaps in the workforce, clarifies the skills in demand, and provides the transition pathway opportunities for individuals to retrain, will make entry or transition into the cyber workforce easier.

Reforms to education and migration could also provide opportunities to address the cyber skills shortage. Streamlining the skilled migration process and establishing more Mutual Recognition of Qualifications Agreements, would make it easier and more attractive for highly skilled cyber security professionals to relocate to Australia.

Elevating Digital Literacy and Technology within school curriculums to ensure a greater cyber-literate cohort, equipping students with relevant foundational skills to make decisions about pursuing a career in cyber security, either through further education or immediate entry to the workforce.

Enduring and adaptive sovereign capabilities

We support a secure Australia, that has advanced, adaptive capabilities to counter cyber threats. However, to achieve this, there is significant work required to understand emerging technologies and address the cyber skills shortage.

To increase the maturity of our sovereign capabilities, the R&D Tax Incentive Assessment model could be updated to specifically account for software and technology development. Local growth and innovation in cyber technology should be incentivised through the use of tax deductions and grants, bringing Australia in line with our international counterparts. We also encourage the Government to recommit to the recommendations set out in the ICT Procurement Taskforce Report of 2017.

Australia needs to leverage international expertise in education and technology to assist our education sector in developing tailored courses to address new technologies, such as quantum computing and AI, to support sovereign growth in these capabilities. The Government should commit to a forward work plan considering education, skills output, innovation for start-ups and SME's.

Advanced cybersecurity built in by design

We support Australia keeping pace with emerging technologies such as artificial intelligence, quantum computing and the internet of things (IoT) where appropriate safeguards and considerations have been taken.

Mandating secure 'by design' principles in the build stage of developing these new technologies could be a valuable policy consideration. Making strong policy decisions at this stage allows businesses to factor in sensible prioritisation of the secure components throughout their systems and associated levels of risk. The Government should be open to considering for example the use of a Software Bill of Materials or the development of a central vulnerability disclosure point across sectors to identify any unsupported software. Advanced cybersecurity measures allowing for secure software and hardware development will require the Government to be bold in the initiatives they pursue.

Greater awareness at the board level of the principles of secure by design should be promoted by technical experts to the members of the board to ensure this understanding can be disseminated clearly to the highest levels of business decision making.

ATTACHMENT A: Answers to 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?

The greatest potential for cyber uplift is in non-critical infrastructure sectors: small and medium businesses and larger businesses in sectors outside of the scope of the SOCI Act. Many such business hold nationally significant information, or significant amounts of personal data, in sectors such as healthcare, real estate and mining. Government could consider federal centralised tokenisation models to reduce the need for organisations to hold sensitive customer documents. Achieving an uplift in cyber security in these businesses will require a sustained focus by Government to raise the awareness of cyber risks across the economy by educating directors and arming small and medium enterprises with the information they need. For example, through targeted education campaigns and guidance materials for these enterprises and engaging with larger companies to improve awareness within their own supply chains.

We believe there is opportunity for Government and industry to collaborate on joint 'missions' leveraging shared expertise to tackle the most pressing cyber issues impacting the nation. This cooperation should reach beyond information sharing and seek to identify significant and emerging threat vectors. The Government could co-locate skilled operational staff from relevant organisations with Government to seek to address some of these issues. The capital city Joint Cyber Security Centres (JCSCs) could serve as a logical base for this joint work.

Legislative & Regulatory

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

We support Government's view that cyber resilience requires an integrated whole-of-nation approach across Governments, individuals, and businesses of all sizes. We believe the Government can achieve this by uplifting the awareness of the risks to organisations large and small. For example, educating the board of directors of larger organisations[1] and arming small and medium enterprise with the information they need to protect their businesses. The more knowledgeable businesses are about cyber risks, the more effectively they can manage those risks.

New or enhanced regulation should only be introduced where it will solve a clearly identified problem. Introducing complex and duplicative regulation, such as by including customer data and systems as a critical infrastructure asset, will not uplift cyber resilience across the digital economy.

[1] For example, by issuing guidance on how directors should consider and mitigate cyber security risk. A similar approach has already been used by the Australian Securities and Investment Commission ('**ASIC**') for the management of climate-related risk. ASIC has provided guidance on how directors should consider climate risk. Such guidance would assist Boards in considering cyber security risk within the generic (and principles-based) approach of director's obligations.

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)?**

Risk Management Program Rules under the SOCI Act apply to critical infrastructure sectors. For other sectors, we believe that the focus should be on education about cyber risks, providing SME's with the tools and support available to help them protect themselves. This includes providing guidance about minimum cyber security standards.

This approach is consistent with our response to the Government's Privacy Review Report, where we proposed that to best address rapid changes in the information security and threat landscape over time, it would be useful to embed desired baseline privacy outcomes within OAIC guidance materials (together with references to key resources such as the ACSC's Cyber Security Principles) rather than within the Privacy Act.

Some industries are well placed to drive the adoption by clients and supply chains of reputable cyber security standards or frameworks like Cyber Essentials, ISO27001 or NIST. At Telstra, minimum data security requirements are flowed through to suppliers contractually and we regularly review and conduct programs of work to help uplift security practices with our supply chain.

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?**

We support harmonising existing data protection regulation and reducing complexity in the storage and protection of data. We view this as critical to being able to successfully secure customer data. However, we do not support including customer data and systems as critical infrastructure under the SOCI Act.

The critical infrastructure and systems of national significance reforms were introduced to the SOCI Act with the intention of protecting and actively defending the critical infrastructure that all Australians rely on.[2] Before introducing further changes to the SOCI Act, the Government should be clear about the problem it is trying to solve. This is to ensure the change is necessary, effective and does not create additional complexity or duplication, or have other unintended consequences.

Like many large organisations, Telstra is subject to several data protection laws and regimes, including the *Privacy Act 1988* (Cth), *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth). Expanding the obligations under the SOCI Act to include data or systems not related to the operation of critical infrastructure will add to the existing complexity around data storage and protection and is unlikely to result in improved cyber outcomes across the economy. It also suggests a siloed approach by

[2] Australian Government, *Australia's cyber security strategy 2020*, p. 6.

Government to the protection of data, noting the data protection proposals previously tabled in the Attorney General's Privacy Act Review Report and Discussion Paper on the Reform of Australia's Electronic Surveillance Framework. We urge the Government to adopt a whole of government and whole of economy approach to cyber security and the protection of data.

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

The *Corporations Act 2001* (Cth) is a principles-based and technology neutral framework that is sufficiently broad to address cyber security challenges and emerging risks.[3] The existing obligations and liabilities are effective and have appropriate enforcement mechanisms.

Telstra supports raising awareness of cyber risks to organisations large and small, however we do not believe cyber specific changes to director duties are required. Raising cyber awareness can be achieved most effectively by educating the board of directors of larger organisations and arming small and medium enterprises with the information they need to protect their businesses. The more knowledgeable businesses across the economy are about cyber risks, the more effectively they can manage those risks.

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

Any new regulation should be clear about the problem it is trying to solve. If the purpose of a Cyber Security Act is to improve cyber security resilience across the whole of the economy or to harmonise existing cyber-specific obligations, it is not clear how the Act will achieve either purpose.

Existing cyber obligations are industry specific, overseen by multiple regulators and often go beyond minimum baseline standards due to the nature of the industries in which they operate. Examples include the SOCI Act for critical infrastructure sectors and security frameworks within the financial services, energy and telecommunications sectors. Harmonising existing cyber-specific standards across these industries within a Cyber Security Act will not improve cyber security outcomes across the economy. However, clarity about cyber specific standards within a sector (such as between the TSSR and SOCI Act for the telecommunications sector) has a clear benefit of reducing complexity for that sector.

3 Refer to Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496, where the respondent (within the financial services sector) was found to have breached certain general obligations under the Corporations Act by failing to have adequate cybersecurity risk management in place

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?**

For the telecommunications sector, there is an opportunity to streamline the Risk Management Program obligation under the SOCI Act and the existing security and reporting obligations under TSSR. This has been recognised by Government and we understand is being considered as part of the ongoing TSSR review.

Further to this there is an opportunity to streamline data protection under one legal framework, such as the Privacy framework. This would mean that any obligations in relation to data protection could be regulated by the OAIC instead of the introduction of further legislation in the form of a new Cyber Security Act or reforms to the SOCI Act.

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?**

Ransomware attacks have seen exponential growth in recent years and businesses may believe they have little recourse but to pay ransoms. Prohibiting the payment of ransoms would provide clarity to victims of cyber-crime and insurers about the options available to them following a ransomware attack. However, it may also be more debilitating for victims of cybercrime, companies and insurers where an entity moves to underground methods to pass the ransom onto cybercriminals. In this circumstance, there are further risks that criminals may threaten to disclose the payment of the ransom and further extort the entity. The Government should consider how to balance these two risks when developing its policy in relation to ransomware payments.

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?**

A strict prohibition would provide clarity to victims of cyber-crime and insurers about the options available to them following a ransomware attack. However, it may also be more debilitating for victims of cybercrime, companies and insurers where an entity moves to underground methods to pass the ransom onto cybercriminals. In this circumstance, there are further risks that criminals may threaten to disclose the payment of the ransom and further extort the entity.

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?**

Government should continue advocating for the importance of incident response plans and having routine back-ups, such that businesses will not feel compelled to pay a ransom.

International

The Department of Foreign Affairs and Trade has led an impressive program of engagement and capacity building on cyber security and critical emerging technology issues. Australian advocacy efforts

by both Government and industry will remain vital in promoting the balance between maintaining the rule of law online and ensuring the continued openness and democratisation of the internet.

Collaboration on operational issues, such as cross-border information sharing, and incident response will become even more important as nation-states increase their use of cyber means to achieve political and economic objectives and in support of kinetic military operations.

Criminal actors continue to scale their tactics and techniques across geographic regions – if a campaign is successful in one part of the world – it will often emerge on the other side of the globe within weeks.

To stay ahead in this environment, there are several key areas of focus ripe for increased engagement, these include cooperation between industry, Governments and academia.

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

   We endorse the view that Australia has a strong reputation as a respected partner, collaborating with and supporting countries in our region, with respect to cyber resilience. Regional cooperation is pivotal in staying ahead of emerging threats, as is listening, and engaging with our neighbours to understand the issues that are impacting them the most and what extra support and capacity is required. This understanding is required to form the basis for meaningful and tangible cooperation.

   The Government could look to leverage its previous experiences delivering capacity building and exercising programs in an ASEAN Regional Forum (ARF) context into the Pacific. These workshops included sessions on cyber strategy and legislative formation and a practical incident response exercise that tested crisis coordination responses at a national level, and between countries during a cascading incident.

   Given the strong internet infrastructure links between the Pacific and Australia, an exercise of this type would be a practical, meaningful means of testing resilience and building trust between Governments and private sector service providers.

   To assist with international outreach on technical issues the Government could look to re-establish national CERT Australia team functionality. CERT Australia was previously instrumental in the formation of regional exercises and capacity building sessions in the ASEAN context. Whilst DFAT has adeptly managed policy and strategic outreach activities with the Pacific, supported by ACSC's international engagement section, a dedicated CERT team functionality could better support the technical uplift, and sharing of indicators of compromise with partner countries.

   Information sharing and external engagement (both domestic and international) are culturally difficult and often lower-priority activities for intelligence agencies to perform, and there is an obvious gap that could be filled by a Government function that operates outside a national-security or intelligence apparatus at an 'unclassified' level by a CERT-like function.

   From a threat-sharing perspective, there may be an opportunity for Pacific Island Governments to connect to the ACSC's Cyber Threat Information Sharing (CTIS) platform and consume feeds of the appropriate Traffic Light Protocol (TLP) status.

Telstra has participated in several of DFATs 'Cyber Bootcamp' workshops which provide hands on experience and training to Government officials from ASEAN countries. This model, which brings together Government, academic and industry experts to discuss technical, security, policy and regulatory approaches in an honest and open environment has proven to be an extremely successful model. We look forward to contributing to future programs and encourage the Government to maintain and expand the program to a greater number of countries.

Further ways Australia can work with our neighbours to build cyber resilience and improve incident response are through the areas of skills, training and awareness, and capacity building.

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

Bilateral agreements, such as those Australia has recently signed in PNG and Vanuatu, provide a vehicle for countries to discuss a range of issues of common interest, including how to develop areas of cooperation and practical solutions to address the evolving nature of our shared security interests, including non-traditional security challenges such as cyber security.

At a regional or multilateral level, there may be an opportunity for Australia to leverage the Pacific Islands Forum (PIF) as a vehicle to further deepen regional approaches to cyber resilience. The PIF expanded the notion of security to include cyber security via the Boe Declaration on Regional Security. This laid the groundwork for the inclusion of cyber threat updates in the recently established Pacific Fusion Centre. We believe there are opportunities to leverage the expertise and regional visibility of Australian private-sector organisations, who could provide updates on tangible and ongoing threats to PIF member-states via the Pacific Fusion Centre or other appropriate mechanisms.

The Quad partnership has established a 'Senior Cyber Group' of leader-level experts who will meet regularly to advance work between Government and industry on driving continuous improvements in areas including adoption and implementation of shared cyber standards; development of secure software; building workforce and talent; and promoting the scalability and cybersecurity of secure and trustworthy digital infrastructure.

Relevant senior industry representation from member-states could be sought to join the senior cyber group where relevant to coordinate and share expertise on key emerging issues. A telecommunications Quad industry working group could be considered, comprised of key carriers from Quad member states.

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?

Standards

Australian Government and industry must work closely together on standards setting. This engagement should include both the developers and users of critical technologies and leverage cyber security and technical expertise within Government and the private sector. Government should seek

to utilise industry in key standards setting to help create an informed and consolidated national approach.

Norms

Certain private sector organisations are well positioned to assist Government in validating if nation-states are adhering to the 11 agreed norms of behaviour under the UN framework of responsible state behaviour in cyberspace. By sharing reporting when organisations become aware of activity that may breach these agreed norms, the Government can more easily assess norm implementation and track breaches. Logical areas for information sharing in line with the agreed norms could include, sharing knowledge of instances where nation-states have targeted critical infrastructure that serves the public, knowledge of positive efforts to protect domestic critical infrastructure, knowledge of misuse of ICTs within national borders and ensuring supply chain security.

Government Security

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

Commonwealth Government departments and agencies have a responsibility to demonstrate cyber security best practices, particularly in leading cyber uplift and resilience across the economy. Although the Government has mandated Essential Eight for all entities, there is no timeline for implementation and the Commonwealth Cyber Posture for 2022 revealed that Essential Eight maturity levels remained low across Government. The number of entities that had exercised their Incident Response Plans every two years was also low. Providing some clarity around the timeline for implementation will encourage greater uptake and ensure appropriate levels of preparedness across Government.

Government could also assess the merits of a secure national network that enables a nationally coordinated threat response and threat visibility, to help protect Government networks.

The Government may consider the viability of using zero-trust architecture within its systems to model cyber security best practice. Zero trust architecture enhances end-to end security, by requiring authentication of identities at every connection request, encouraging cyber security best practice. The US has introduced a strategy to ensure that all federal Government systems are modernised by migrating to a zero-trust architecture framework. The UK National Cyber Security Centre has also released guidelines to help implement zero trust architecture. It may be worth exploring whether the ACSC can release similar guidelines or provide actionable advice on implementing zero trust architecture for Government systems in Australia.

Threat Sharing and Reporting

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

Like all Australian businesses, we face a constantly evolving threat environment. As an ISP we have unique insight into the types of threats that are facing the nation online. The scale, diversity, and pace of transactions and communications across Telstra's networks provides a rich, unique map of the Australian threat environment. The threats we see targeting our customers range from the

sophisticated, emanating from well-resourced adversaries, to high-volume low sophistication attacks that target vulnerable Australians and are often financially motivated.

Telstra works with public and private entities to understand, locate and identify anomalous and malicious indicators in network traffic metadata and inform our customers when this activity is identified in line with our privacy policy.

CTIS

The launch of the Cyber Threat Information Sharing (CTIS) platform was an important first step to enable Government and industry to share key indicators on current threats.

Telstra consulted extensively with ACSC during the creation of the new CTIS platform. Telstra actively shares indicators via the platform related to activity we have observed that meets a designated threshold. Shared activity must be sufficiently long running that the information is still actionable by the time the CTIS community consumes it, and the activity must be relevant to, and appropriate to be shared with the CTIS community.

To further strengthen CTIS attention should focus on improving the quality of indicators shared across the platform. Currently many organisations are investing resources to validate CTIS outputs as part of responsible due diligence activities before they are applied in an organisational context.

By validating the indicators, (or by providing both 'high-priority' validated and 'lower priority' unvalidated feeds) the ACSC can improve confidence in CTIS feeds, reduce validation workloads on consuming organisations and increase the usability of the platform for small-medium organisations. This human-validated stream should include the most important, timely and actionable threat intel indicators for action.

National Information Exchange

In-person threat information sharing sessions have traditionally been a vital means to establishing trust in the threat intelligence community. Previously National Information Exchange (NIEs) and the more recent state-based efforts, (i.e. the NSW Operational Intelligence Exchange (NOIE)) have proven to be useful forums to receive organisational updates from industry and Government partners and gain visibility of the threats facing the wider economy.

Covid-19 understandably impacted the ability for these forums to held, but now as restrictions have eased, the size and scale of NIEs should return to pre-covid formats. Namely a national meeting held in Canberra on a six-monthly basis that brings together organisations from across the nation with developed threat intelligence capabilities and threat visibility. Sessions should include the opportunity for Government and industry to share two-way discussions in an open and trusted forum – with relevant representation from Government and industry technical experts.

Supporting meetings with a broader range of sectors with less developed capabilities could be held in JCSCs in regional capitals.

Trusted Information Sharing Network (TISN)

The TISN is a partnership forum, comprising industry and Government, where members can engage on all-hazards approaches to improving the security and resilience of critical infrastructure. Government has recently promoted the TISN as the key touchpoint for industry for cooperation on cyber and critical infrastructure issues.

It can often be unclear to industry where the TISN fits within the broader Government cyber and security apparatus. For example, clarity around how collaboration with Government under the TISN differs to engagement via the ACSC would be beneficial, including which issues belong to each mechanism.

Government could also work to improve legal clarity concerning the disclosure of telecommunications data to non-law enforcement agencies, such as the ACSC, for security and remediation purposes.

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?**

   Telstra maintains an established and proactive and trusted two-way relationship with the ACSC.

   We believe that an explicit obligation of confidentiality by the ASD and ACSC would improve engagement with organisations that experience a cyber incident and do not currently have a strong working relationship with the ASD/ACSC. This would allow industry to feel confident in providing information relating to a cyber incident and facilitate working together immediately on responses. However, an explicit obligation of confidentiality may not be sufficient in the circumstances where an organisation has a legal obligation to disclose certain information to a regulator. In this instance, a safe harbour provision which released the organisation from regulatory prosecution would allow for more open and transparent dialogue between Government and industry.

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?**

   Improving the public understanding of the nature and scale of ransomware and extortion through education, uplifting skills and providing the necessary tools to respond to a cyber incident can assist the public in being aware of the risks and better responding to ransomware attacks. Increasing notification and reporting obligations will not necessarily achieve that same outcome and does not account for the notification fatigue that entities will and in some instances already face. If the regime is expanded to require mandatory reporting of ransomware or extortion demands, more focus needs to be placed on harmonising the reporting method. A recommendation is to provide a central reporting portal, such as ‘ReportCyber’ and assign the triaging function of reports to the ACSC.

   More concerted efforts need to be made at education campaigns focusing on ransomware to improve the public understanding.

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

Telstra employs automated threat blocking through our Cleaner Pipes initiatives which involve significantly upscaling our Domain Name System (DNS) filtering, where millions of malware communications are being proactively and automatically blocked every week as they try to cross Telstra's infrastructure. This action reduces the impact of cyber threats on millions of Telstra's customers including stopping the theft of personal data, financial losses, fraudulent activity and users' computers being infected with malware. Additionally, Telstra's SMS Filter uses automatic machine scanning to pick out suspicious content such as malicious links and combines this with other patterns and characteristics to block an unprecedented volume of scam SMS. Since launching, it has blocked close to 230 million SMS messages (April 2022-February 2023). Such a model can be useful when used in conjunction with organisations that have similar capacity, to expand the reach of the filter.

Skills and Employment

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

Although steps have been taken towards addressing the cyber skills shortage, an approach that focuses on harmonising existing opportunities across states and territories would be useful. Each state and territory has implemented their own initiatives to grow cyber skills and education. The Government's STEM agenda has also seen increased momentum within the tertiary education sector, which will result in specialised cybersecurity graduates within the next few years. Leveraging the momentum and mapping the various initiatives in a central portal will help to identify the gaps in the workforce.

The portal can also clarify the skills in demand and can provide opportunities for individuals to retrain through transition pathways. Government and industry have through partnerships or their own ventures attempted to address the cyber skills shortage, but information is not centrally available in one location. We suggest, rather than creating another framework, there is greater utility in providing a consistent foundational list of skills and qualifications that are in demand.

The aim of a tailored approach should be to simplify the offerings across the country, particularly where there are discretions for example in the costs associated with a Certificate IV in Cybersecurity between Victoria and Queensland (approximately $9000 and $13,000 respectively). Ideally, this portal should be easily navigated by students and parents, teachers and career counsellors, people looking to reskill or undertake further learning or training. Creating something equivalent to myfuture.edu.au for cyber security, bringing together various offerings should be the product of the tailored approach that the Government needs to undertake to uplift cyber skills.

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

Education

Stronger partnerships between educational providers and employers helps to equip graduates with the skills our workplaces need. At Telstra, we are currently working with five Australian universities to enhance student learning through providing input into curriculums, industry placements and

integrated work experiences, research and innovation opportunities, and early access to career opportunities.

According to an OECD report, the proportion of new students entering STEAM-related bachelor's degree programs in Australia sits at 21%, compared to 27% for other OECD countries. Elevating Digital Literacy and Technology within school curriculums to equate to English, Mathematics and Science, will ensure a greater cyber-literate cohort, equipping students with relevant foundational skills to make decisions about pursuing a career in cyber security, either through further education or immediate entry to the workforce. To accomplish this, it is vital that teachers receive appropriate professional learning support to be able to teach the curriculum confidently.

This is mutually beneficial to industry, who are eager to provide on the job training for a return investment in prolonged employment. Industry can prepare for such roles, by considering the appropriate roles and skills that junior employees will be able to complete, without significant risks to the business. Government can assist businesses willing to provide on the job training/internships by funding these initiatives or covering the cost of associated training or certification. Students that follow this career pathway can develop competency in skills quicker and the value to the business is immediately apparent.

Immigration

Australia's migration pathways make it difficult to attract and retain talent to assist with the cyber skills shortage. There are many avenues to enter in the cybersecurity industry, some of which may not be recognised under traditional tertiary education courses. Lowering the number of years of work experience required in a relevant field, where the applicant does not have a university degree, could allow easier entry of global talent to fill the skills shortages in Australia.

Mutual recognition of certifications for highly skilled cyber security professionals in countries with established and rigorous certification programs should be considered. Currently senior practitioners from the UK/US/NZ are regularly forced to sit expensive but comparably low-level Australian technical courses before they are granted skilled visas, this serves as a disincentive when other nations are quicker to recognise their existing accreditations and skillsets. Where possible, broader industry certifications should also be recognised across similar standards internationally to lower barriers to entry.

Government could also look to reconsider the removal of 'ICT security specialists' from the Skilled visa processing priorities list, formally the Priority Migration Skilled Occupation List (PMSOL). Whilst organisations are still able to sponsor highly skilled workers under the Global Talent Employer Sponsored (GTES) program, there is a limit of 20 available sponsorships across an entire organisation (including non-cyber specific roles).

Accreditation

We consider than an accreditation framework relating to the entire cybersecurity workforce may not be necessary. For certain sectors and specialised fields, there may be utility in an accreditation process, but this should be managed on a sector-sector basis and by sector regulators. This will require a governing body to maintain the framework and change within this sector will evolve, quicker than the administrative processes required to amend the framework. The Government has many

opportunities, listed above in the education and immigration space to explore in support of the cybersecurity workforce.

Incident Response

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

The Government should develop and lead regular national cross-sector crisis response exercises to test the national Cyber Incident Management Arrangements (CIMA). Whilst Government has held sector specific exercises, a cross-sector exercise is needed to test interdependencies and incident response processes between sectors and Government. Specifically, scenarios exploring the sustained disruption of essential systems and associated services, affecting CNI and with potential national security implications. This would allow Government and industry to establish mutual expectations and thresholds for a nationally significant cyber crisis event. Running these exercises at a regular cadence e.g., annually, would encourage continuous improvement, build strong partnerships and provide a mechanism for regular measurement of industry-wide cyber maturity. Exercise findings should also inform future policy development and strategy implementation progress measurements.

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

Creating a single reporting portal for cyber incidents would be beneficial where the practical difficulties around different reporting thresholds and confidentiality restrictions between the ACSC and regulators can be overcome. 'ReportCyber' currently allows for the reporting of cybercrimes, vulnerabilities and cyber security incidents. This could be expanded to include other reporting obligations as new technologies and threats emerge (for example, ransom payments). It will be more difficult to incorporate mandatory data breach notifications to the OAIC within the portal given the difference in threshold and purpose for this reporting requirement.

Consideration should also be given to appropriate information-sharing restrictions between the ACSC and regulators; and a safe harbour provision which released a notifying organisation from regulatory prosecution of a cyber incident to allow for more open and transparent reporting of cyber incidents.

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

A model similar to the US Cyber Safety Review Board (CSRB) would be an effective post-incident review and consequence model. The scope of the CSRB extends to both Government and industry systems, threat activity, vulnerabilities, mitigation activities and agencies responses. This could be housed within the recently announced Office of Cybersecurity within the Department of Home Affairs.

The Board should be convened with both Government members and industry representatives. These members should have access to all relevant information, with appropriate safeguards in place, so

they can provide an unfiltered view of events that led to incidents and the aftermath. Consideration should also be given to the scope and impact of an incident, before a Review Board is engaged, and these parameters should be clear.

Awareness, SMB & EU Security, Secure-by-design

15. 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?

Cybercrime Victims

Directing cybercrime victims towards expert help that provides streamlined, timely assistance is vital. Both industry and Government have a responsibility to be transparent about who to contact when an individual believes they are the victim of cybercrime. All organisations also need to ensure they use secure digital communication systems which provides consumers the protection they want.

The Government could also consider increasing support to organisations like IDCARE to rapidly increase support available to victims. Education, whether through formal channels as discussed at question 12 or industry and Government campaigns, is the key factor in improving cyber best practice and knowledge to create a more cyber-literate population.

SME

Although aware of the need to manage the inherent risks of cybersecurity, small businesses can lack the expertise, skills, and resources to achieve this. The Government needs to continue having a sustained focus in the small business space and engaging with larger companies that are driving innovation. The Government should continue to focus on educating smaller businesses of the cyber risks and threats that they are faced with and give them access to tools to defend themselves.

For example, Telstra partnered with Cynch Security and AustCyber to offer a free cyber security fitness program pilot to help up to 200 SME's understand and improve their cyber resilience, particularly useful for those supporting critical supply chains. The self-service program helps businesses understand gaps in their existing cyber security measures, self-identify as being within the scope of the SOCI Act, help follow clear programs of work to uplift and provide reporting capabilities to assess how well they are doing.

Large businesses need to be bold in their efforts, willing to assist in meaningful ways and receive funding support from Government to educate SME's.

For example, 'Cyber Wardens' is a program currently in development which is building a simple education tool designed to develop a cyber-smart small business workforce. It aims to become Australia's first cyber safety workplace certification or micro credential for the small business sector. It is an initiative of the Council of Small Business Organisations of Australia, supported by an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre and delivered by 89 Degrees East.

When focusing on education campaigns that target small businesses, there needs to a human-centred approach informed by experts on culture change, not just communications. Leadership in small business is pivotal in directing strong security practices and awareness.

As part of the cyber strategy, to understand the practical working concerns of small businesses, we suggest setting up a quarterly forum of key leaders to address issues and provide accountability as a measurable tool.

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?

Australia needs to do more to keep pace with evolving cyber security technologies and to encourage the uptake of services and technologies nationally. As a first step, we recommend mapping the cyber security professionals that will be required to facilitate new technologies and aligning these with the suggestions made above for addressing the skills shortage at Question 12.

Much of the innovative technology in development is occurring overseas and the Government needs to commit to an infusion of international talent and partnerships, particularly attracting those that have experience in scaling up businesses. Additionally, investing in more research chairs at university can encourage more sovereign innovation to develop. Mandating secure by design principles in the build stage of developing these new technologies could also be a valuable policy to consider.

The Government could consider updating the R&D Tax Incentive Assessment model to specifically account for software and technology development. A Tech Council Report found that in 2021, Australia ranked lower for measures of domestic technology innovation and creation, ranking 11th out of 38 for the R&D budget and 20th out of 38 for SME tax subsidies. The Government can contribute to the maturing of the cyber security ecosystem in Australia by further incentivising growth through targeted tax incentive frameworks. Comparatively, Singapore has elevated its scheme by introducing a new Enterprise Innovation scheme to provide up to 400% tax deductions for businesses working on qualifying activities to boost innovation. Following international examples, the Government should review the R&D incentive to explore whether such a significant boost could be administered

Supply Chain and Emerging Tech

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

Australia's approach to emerging cyber security technologies should be open, innovation-driven, and cautious. There are many unknowns of emerging technologies, their capacity and potential to improve our lives but also the significant risks that may unfold. Topics such as AI, quantum computing and "deep fakes" all present challenging problems for policy makers. The best path forward is to ensure Australia continues to engage with likeminded neighbours, increase our understanding and knowledge through effective dialogue and remain cognisant of emerging risks.

Quantum technology is an area of emerging tech that the Commonwealth Scientific and Industrial Research Organisation (CSIRO) predicted in October 2022 would reach $6 billion by 2045, generating more than 19000 jobs. The core issue is that quantum computing may be able to crack the digital encryption which underpins modern information and communications infrastructure. In

response, progress has been made in the US for example towards developing post quantum cryptography methods and standards development to assist with the inevitable transition that is coming. Similarly, Australia's approach to future proofing these technologies needs to align with boundaries set by standards, balanced with driving innovative thinking by creating alternate solutions.

The Australian Government has commenced work towards a National Quantum Strategy and there are periods of uncertain transition ahead as technology develops. To position ourselves well, Australia needs to coordinate internationally with leading quantum researchers and academia, assist in developing standards and understanding the supply chain. A greater uptake of graduates in quantum technology fields is necessary, but the importance of this technology is undervalued, just as cyber security was decades prior. Using the lessons learnt from the emergence of cyber security as a field and the equivalent increase in tertiary courses in recent years, tailored course considerations should be in the pipeline. Leveraging expertise internationally in education and technology space, will assist with these preparations for Australia's education sector.

International supply chain concentration risk remains a significant concern., as occurred with the global shortage of semi-conductor chips. There needs to be greater awareness of understanding of the scope of vendor risks, which means regular audits of vendors is important. To ensure diversity in the supply chain, Governments should consider the cost benefits of establishing longer-term contracts with diverse trusted key suppliers to build additional resilience. Some Governments are increasing domestic manufacturing capabilities and bolstering leadership in the semi-conductor industry as a means of future proofing against any disruptions, such as the US through the CHIPS and Science Act. An immediate target amongst like-minded Governments, key manufacturers and network operators, should be to identify and pool resources (subject to competition law compliance) into manufacturing these key or 'niche' components that are currently only produced in high-risk locations. Whilst market-driven approaches, including Open RAN drive an important medium-longer term and cost-effective component manufacturing process, vendors will be profit, not national security driven and may not choose to produce critical products where they do not possess a comparative advantage.

The Government should explore the viability of a Software Bill of Materials framework to increase software component transparency. In the US, this is a nested inventory which provides a list of components that makes it clear to software product buyers, what is included in the products they are purchasing. This leads to quicker vulnerability patching as entities have greater awareness about the specific components in their networks. As technologies develop, vetting software components that go into products could be considered a quick win in future proofing against any risks and encourage secure software development.

Across sectors, the Government should encourage industry to develop a central vulnerability disclosure point to identify any unsupported software. Businesses should factor in sensible prioritisation and have awareness of the impact of different software components through their systems and associated levels of risk. On a Government level, a pilot of a Government Coordinated Vulnerability Disclosure policy could be helpful to allow private individuals to identify and report vulnerabilities in ICT systems to an approved framework. The partnership between industry and Government must continue to strengthen as a necessary future proofing tool against cyber security technologies by investing in bold initiatives.

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?

The Government has significant potential to use procurement to support and encourage the Australian cybersecurity ecosystem. Full access to public sector procurement data would provide insight and intelligence into Government needs. This data could enable those SMEs interested in selling to Government, the opportunity to effectively compete with larger entities.

The Government could also consider minimum cyber security requirements for vendors participating in Government procurement processes.

A reform in Government procurement processes may be necessary, particularly in the pre-tender engagement stage to allow for productive market engagement with SME's, that allows Government to challenge and absorb some risk by leaning into the innovative solutions they may provide. The ICT Procurement Taskforce released a report in 2017, with a commitment from the then Government to increase by 10% the annual ICT spend on SME's. Considering the implementation and progress that has been made on the 10 recommendations from the Taskforce would be a first step to improving procurement processes.

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

The Strategy should recognise the immense benefit that emerging and new technologies will have, balanced with the inevitable need for more boundaries, standards and potential legislative requirements in the future.

Where international standards exist or are in the process of development, the Strategy should encourage the Government to create standards that align internationally.

The European Union is also considering a Cyber Resilience Act, which creates requirements for hardware manufacturers, software developers, distributors and importers who place digital products or services on the EU market. These requirements include an appropriate level of cybersecurity, not selling products with known vulnerabilities, security by default configurations, protection from unauthorised access, limitation of attack surfaces and minimisation of incident impact. The Government should closely follow the development of legislation and look to lessons learnt to consider whether similar legislation would be appropriate in an Australian context.

Requiring security by design at the build stage of technology that is yet to be developed is a minimum level commitment that should be able to protect against some unknown variables. Concurrently, there needs to be greater awareness of secure by design at the management and board level. We suggest that technical representation on Boards is required as technology emerges to ensure a base level of understanding permeates to the top layers of business. Further the Strategy should encourage using threat intelligence to have clear visibility of threats and attack vectors to ensure they are accounted for in the design stage.

The Strategy should lean into the benefits offered by Artificial Intelligence and Machine Learning in assisting with automating processes to detect malware and anomalies outside normal behaviour

patterns. Better detection of cyber-attacks is possible through more accurate predictions leading to faster response times. Concurrently, it is important that the Strategy promotes processes that are known to work to ensure there are no single points of failure for example having data centres split across multiple geographic locations and having variations in technology stacks.

Assessment and Evaluation

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

The Government could invest in improved data collection, research and analysis to underpin the impact of uplifting national cyber resilience. This should include periodic assessments of the cyber security maturity of public and private sector organisations. Further we suggest correlating investments made to outcomes specifically intended for uplifting national resilience, providing transparent and comparative reporting, available to the public. ACSC/ASD could consider the establishment of a specialist data analytics and communications team to help design quantifiable threat data frameworks. Through the 'ReportCyber' portal, the Government has access to a pool of information, which should be anonymised and used to identify common trends and patterns. This work should also seek to inform evidence-based policy formation across Government.

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

We suggest that an external advisory committee is once again established to assist with implementing the Strategy. This will allow industry to raise concerns with senior officials in a timely manner, as initiatives are being rolled out.

As in the previous Strategy, the continued use of performance metrics for all initiatives developed under the Strategy will be a useful evaluation measure. Progress, monitoring and reporting will allow for evaluation that focuses more heavily on outcomes. We welcome the continuation of a regular cadence of publications updating the public on Strategy progress, particularly on the forward work plan for emerging and future technologies.

Specialist skills are often required for data collection, analysis and evaluation. Many international and domestic public sector counterparts have specialist resources dedicated to evidence and evaluation. For example, the UK National Cyber Security Centre has an evidence unit that contributes to the public evaluation of the cyber security strategy. Investing in this capacity to bring together a dedicated team will assist ongoing public transparency and measurable outputs.