2023-2030 Australian Cyber Security Strategy: Discussion Paper

PwC Submission

April 2023

pwc

15 April 2023

Consultation into the 2023-2030 Australian Cyber Security Strategy

To whom it may concern,

PwC Australia welcomes the opportunity to provide this submission to the Department of Home Affairs' consultation into the 2023-30 Australian Cyber Security Strategy - Discussion Paper (Discussion Paper). We commend the Federal Government for its ongoing commitment to enhancing Australia's economy-wide cyber posture and its ambitious goal to make Australia the world's most cyber secure nation by 2030.

Given the breadth of our cyber-related work and the diverse range of clients we work with across multiple sectors, PwC has unique insights into the opportunities and challenges the 2023-30 Australian Cyber Security Strategy (the Strategy) can serve to address. We trust this contribution will support the government's overall goal of ensuring Australian institutions, organisations and, most importantly, citizens, are cyber secure and able to fully realise the myriad opportunities digitisation offers.

The new Strategy, and the longer-term approach it proposes, presents a unique opportunity to build on the significant work that has already occurred in the legislative and regulatory space - notably reforms to Australia's critical infrastructure regime - and better harmonise cyber obligations for Australian organisations. Ultimately, such harmonisation will serve to reduce regulatory complexity and duplication and help Australian organisations achieve greater clarity in meeting their cyber obligations. It is an opportunity to move cyber beyond compliance and promote secure-by-design principles, from classrooms to boardrooms.

Please note we have not responded to all Discussion Paper questions, focussing on those where we believe our submissions will be of most assistance.

Again, thank you for the opportunity to contribute to this important consultation. If you have any queries or would like to discuss this submission further, please do not hesitate to contact me via phone or email.

Yours sincerely,

[redacted]

Robert Di Pietro

PwC Australia Partner
Cyber Security and Digital Trust Lead

[redacted]

Contents

Executive summary

In a world where the physical and digital continuously overlap, where almost every system and service we take for granted is connected, where we literally carry the internet in our hands, cyber security has never been more important.

Since Australia's first cyber security strategy was launched in 2016, our reliance on digital systems and the cyber threat environment have evolved significantly, largely driven by the COVID-19 pandemic and the accelerated digitisation it entailed. And, while the pandemic served as a catalyst for a mass migration to working and communicating online, it also resulted in a significant increase in malicious cyber activity. This has seen the amount of reported cyber crime in Australia increase 13% year-on-year since 2020, with no sign of abating.[1][2] This trend has been starkly highlighted over the past year, with major cyber attacks on three prominent companies in Australia truly bringing home to citizens, organisations and policy makers the vital importance of bolstering Australia's cyber defences.

Given the rapid changes in the cyber environment, this consultation into the 2023-30 Australian Cyber Security Strategy (the Strategy) is timely. Not only does it provide an opportunity to build on the work undertaken as a result of the previous strategy, notably significant reform of Australia's critical infrastructure regime, it will also facilitate a 'longer term' view of bolstering our nation's cyber posture. This holistic approach touches on all facets of cyber security, from technical protections and regulatory policy, right through to educating people and building the skills pipeline. Furthermore, given this process is occurring concurrently with the consultation into reform of the Privacy Act 1988 (Cth), there is an opportunity to achieve greater regulatory harmonisation, consistency and clarity, especially in relation to data protection in Australia. Taking such an approach will ultimately reduce duplication and support organisations in their cyber uplift journeys. It is also heartening to see a number of other inquiries and initiatives noted in the Discussion Paper, to be considered in conjunction with the Strategy, including digital identity, the National Plan to Combat Cybercrime and the Digital Platform Services Inquiry. By breaking down siloed processes across Australia's cyber ecosystem, there is an opportunity to implement holistic and clear solutions economy wide for the benefit of all Australians.

This submission aims to strike a balance between the need to uplift Australia's cyber defences right across the economy - from government to big business, to small business and to citizens - and the potential impacts and unintended consequences this could have if not carefully considered. We believe that key to achieving the four key aims of the Strategy will be a focus on enhancing public-private partnerships. Taking such an approach will not only drive improved threat intelligence sharing, threat response and sovereign capability, it will embed a culture of shared responsibility, which is essential in the cyber ecosystem. We often hear the refrain that "cyber security is a team sport", and we believe this Strategy, if implemented correctly, has the potential to truly bring this sentiment to life. Finally, we note the Strategy presents a key opportunity for the Federal Government to lead from the front and establish itself as a national cyber security exemplar. This is essential if Australia is to become the world's most cyber secure nation by 2030

To this end, three key themes run through this submission:

1. The **opportunity for enhanced trust and value** building the Strategy can present for the Australian Government, organisations and the broader community.
2. The opportunity the Strategy presents for **harmonisation of cyber-related laws and regulations**, reducing complexity and regulatory burden.
3. The practical challenges organisations may face if the Strategy does not **strike the correct balance between sustainable uplift and increased regulation**.

[1] Annual Cyber Threat Report
[2] ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

Our response to the Discussion Paper questions

We have considered the questions presented in the discussion paper and, where applicable, have presented key advice and recommendations for consideration.

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?

As previously noted, the Strategy presents a significant opportunity for Australia to establish a clear and coherent longer-term approach to addressing a range of cyber-related issues that impact our nation. To this end, we are supportive of the four key areas upon which the government has placed its focus, helping ensure:

- A secure economy and thriving cyber ecosystem
- A secure and resilient critical infrastructure and government sector
- A sovereign and assured capability to counter cyber threats
- Australia is a trusted and influential global cyber leader, working in partnership with our neighbours to lift cyber security and build a cyber resilient region.

We believe to achieve these goals, there are four key areas requiring significant focus, which we touch on below and throughout this submission. These include:

- Increased focus on building public-private partnerships
- Improved legislative and regulatory clarity and harmonisation
- Building a skilled and diverse cyber workforce through education and incentivisation
- Supporting homegrown cyber businesses and innovation to enhance sovereign capability.

Public-Private Partnerships

To bolster economy-wide cyber defences, strong public-private partnerships (PPPs) are essential. Such arrangements not only foster greater transparency and information sharing, they also serve to build trust between public and private institutions. As noted by the US Cyber and Infrastructure Security Agency (CISA): "Information sharing and cooperative action – across both public and private sectors – is essential to our goal of raising the nation's collective defense. The private sector owns and operates a majority of our nation's critical infrastructure, and partnerships between the public and private sectors that foster trust and effective coordination are essential to maintaining critical infrastructure security and resilience".[3]

Globally, CISA has been a frontrunner in the move towards enhanced PPPs and provides a good model for Australia to follow. Notably, CISA's Joint Cyber Defense Collaborative (JCDC), which was established in 2021, brings together organisations and operators from across the public and private sectors, including state, local and international governments, and industry participants including service providers, infrastructure operators, cybersecurity companies and other companies across critical infrastructure sectors.[4] Working together, these organisations proactively gather, analyse and share actionable cyber risk information,[5] with this collaborative approach recognised for its ability to quickly respond and provide guidance in relation to significant cyber threats, such as the Log4j event of 2021.[6]

While some steps towards enhancing PPPs in Australia have been made, notably via the establishment of the Cyber and Infrastructure Security Centre (CISC) and the Australian Signals Directorate-led (ASD) Cyber Threat Intelligence Sharing (CTIS) program, more work is required in this space. Though still young, the CISC has proven to be a uniting force for entities captured by Australia's expanded critical infrastructure regime, working hand-in-glove with industry to provide timely guidance and support in the implementation of cyber uplift programs. And since it was launched in 2021, the CTIS program has seen about 28,000 indicators of compromise (IOCs) shared.[7] Therefore, we submit that a key focus of the Strategy should be to build on the early success of the CISC and to continue to enhance the operations of the CTIS, ensuring both are properly resourced to carry out their functions effectively now and into the future.

[3] Partnerships and Collaboration | Cybersecurity and Infrastructure Security Agency CISA
[4] JCDC FAQs | CISA
[5] Data and public-private partnerships are the future of cybersecurity
[6] Officials say Log4j response proves out promise of new public-private partnership | Federal News Network
[7] The Commonwealth Cyber Security Posture in 2022 | Cyber.gov.au

Legislative and regulatory clarity and harmonisation

To alleviate compliance burden for organisations and to create a more streamlined set of directions for Australian organisations to follow in relation to cyber security posture and practice, we submit that a cornerstone of this reform process should be a focus on better harmonisation of Australia's cyber-related regimes. We also believe, where possible, this should be supported by a clear and prescriptive approach, either through legislation or the guidance underpinning it. Currently, there is a patchwork of cyber-related obligations across multiple legislative and regulatory regimes, resulting in significant duplication and a lack of clarity. However, by taking a consultative approach with affected organisations, an opportunity exists to identify and remediate specific pressure points, proactively encouraging realistic and sustainable uplift. As previously mentioned, this opportunity to create a holistic and integrated regulatory framework must also consider other consultations and inquiries currently underway, an approach we are pleased to see reflected in the Discussion Paper.

Building a skilled and diverse cyber workforce

Australia has a significant cyber skills gap, a problem that has been acknowledged by the government and industry alike. This is not a problem confined to Australia but as our reliance on digital systems continues to increase, it is an issue that needs to be dealt with now to mitigate further shortages into the future. Furthermore, when considering the cyber jobs that need to be filled now and those that will need to be filled in the future, skills transferability and uplift will need to be a focus, given some of the jobs of today will be automated in the future. There are various levers that can be pulled, focussed on education, migration and accreditation, that can help alleviate the cyber skills gap. Encouraging more women into cyber-related careers should also be a focus of the Strategy, noting women represent just 17% of the national cyber workforce.[8]

Enhancing sovereign capability

Australia's sovereign cyber industry continues to grow and, in terms of cyber research and development, our nation produces innovative and novel solutions to help solve complex cyber problems. However, it is often the case that to scale up or commercialise, Australian companies have to look overseas for funding and procurement opportunities. Therefore, more efficient policies and initiatives should be established to help ensure homegrown talent and technologies are supported domestically. Key levers to build this capability relate to government procurement and innovation procurement, which are explored in this submission.

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

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

Over the past several years Australia's cyber-related legislative and regulatory environment has undergone significant change. This is ongoing, with a number of related consultations and inquiries occurring concurrently to the development of the Strategy, most notably the ongoing review of the Privacy Act. Therefore, when considering further legislative or regulatory reforms, these consultations and inquiries - and the potential duplication that could occur - must be carefully considered. Furthermore, we note there are few 'mandatory operational cyber security standards' operating across the economy. This is largely due to the principles-based approach that has been taken in relation to cyber security and, if mandatory standards are to be enacted, more prescriptive guidance should be provided.

In relation to cyber security, the most significant reforms we have seen over the last several years have been to the *Security of Critical Infrastructure Act 2018 (Cth)* (SOCI Act). Many of the sectors captured under the SOCI Act are also highly regulated via sectoral cyber-related regimes, for example, the financial services sector also has cyber-specific obligations under the Australian Prudential Regulation Authority's information security (CPS 234) and the incoming operational risk management (CPS 234) prudential standards. To meet their obligations under the SOCI Act, many organisations have had to undertake significant and costly cyber uplift programs, which will require continuous maintenance and review. Furthermore, these reforms have occurred against a backdrop of difficult economic conditions and a national cyber skills shortage. Therefore, we submit that the critical infrastructure regime should be given more time to mature before additional amendments are made to enhance its operations. This is important because the new regime is still young - the entire raft of SOCI obligations only came online in February, and the first round of Risk Management Programs (RMPs) and annual reporting to the Department of Home Affairs will not occur until later this year. From a regulatory perspective, we submit it would be prudent to allow sufficient time for critical infrastructure capabilities to develop before making significant amendments, with a greater focus on helping captured entities benchmark with peers to help drive further uplift. A good

[8] Women critical to future of Australia's cyber security: report - RMIT University

example of how such a model operates in practice is the Australian Energy Sector Cyber Security Framework (AESCSF), one which could be broadly replicated across different sectors.

A better practice framework: Australian Energy Sector Cyber Security Framework

The Australian Energy Sector Cyber Security Framework (AESCSF) has been developed for the Australian energy sector, enabling Participants to assess, evaluate, prioritise, and improve their cyber security capability and maturity. The AESCSF leverages existing global industry standards, tailored for the Australian energy sector in a way that aligns with existing policy and guidelines like the Australian Privacy Principles and Australian Cyber Security Centre's Essential Eight.[9] Furthermore, as noted in the AESCSF overview, "the Framework could be used by any organisation wanting to assess their cyber security maturity and capability; however, it is particularly relevant to those who operate critical infrastructure or operational (OT) assets".[10] Central to its operation is the Criticality Assessment Tool (CAT), which determines the criticality of each Participant relative to peers. The CAT has three versions for electricity, gas and liquid fuels sub-sectors, which facilitate benchmarking and encourage Participants to stay aligned in maturity with their peers. The annual AESCSF programs have also included sector-wide benchmarking allowing energy organisations to understand where they sit amongst their peers.

There will also be a key role for Australia's Cyber Security Coordinator (the Coordinator), when appointed, to act as a 'clearing house' for cyber-related legislation and regulation in Australia. We submit that, rather than further legislate or regulate, there is a clear mandate for the Coordinator to develop a public central repository of all cyber-related legislation and regulation currently in place across the economy, breaking it down sectorally to reduce confusion and ease the burden of compliance duplication. This would, in effect, allow organisations to devote more time and resources to cyber uplift as opposed to navigating the complex legislative and regulatory environment.

As previously noted, the ongoing review of the Privacy Act should play a key role in the development of the Strategy in relation to the protection of personal information (PI). There is an opportunity to focus such efforts on the harmonisation of Australia's PI-related regimes, supported by a clear and prescriptive approach, noting that we believe any regulation pertaining to PI breaches should stay firmly within the remit of the Office of the Australian Information Commissioner (OAIC). However, there is a key role for the Strategy and the Coordinator to play in terms of helping set clear directions for cyber uplift, especially for small and medium enterprises (SMEs), and the essential cyber practices that should be prioritised to bolster protections. For example, the Essential Eight, published by the Australian Cyber Security Centre (ACSC), has been an effective tool to educate the market on what is 'essential' to mitigate a cyber security incident.

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?*

Reforms to Australia's critical infrastructure regime have been significant and are world leading, as evidenced by the recently released Massachusetts Institute of Technology Cyber Defense Index 2022/23, in which Australian ranked number one in the world among countries showing the greatest progress and commitment to enhancing cyber security.[11] At PwC, we have worked closely with a number of critical infrastructure entities to ensure they meet their obligations under the SOCI Act and have witnessed firsthand the commitment and significant investment these organisations have made to help ensure compliance. Therefore, as outlined above, we do not believe further reform should be considered at this stage, especially in relation to the definition of 'critical assets' capturing customer data.

We submit that protection of 'customer data' primarily relates to personal information and so is an area that should remain in the remit of the Privacy Act, which is under review and may undergo significant reform. Adding 'customer data' into the realm of critical infrastructure would only serve to duplicate already existing obligations and, in the event of a breach, could have the impact of 'double penalising' captured entities and adding to administrative burden. This could also have the unintended consequence of stifling transparency, resulting in impacted organisations failing to report potential breaches due to the potential severity of the penalties. This is not without precedent. In 2021, the OAIC released a statement in reaction to some organisations failing to report potential data breaches due to ransomware attacks, stating: "It is insufficient for an entity to rely on the absence of evidence of access to, or exfiltration of, data to conclusively determine that an eligible data breach has not occurred".[12]

In terms of amending the SOCI Act to include 'systems', further clarification is required. 'Systems' is a very broad term and, if adopted, clear and prescriptive guidance would have to be provided to define what constitutes systems, some of which may already be captured. It could be useful to consider the CISA definition of 'protected systems', as contained in the US Critical

[9] Australian Energy Sector Cyber Security Framework (AESCSF)
[10] Ibid 9
[11] Australia number 1 in cyber progress
[12] Playing dumb no longer an option against ransomware reporting

Infrastructure Information Act 2002, which relate to "any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage".[13]

One area of enhancement which could be considered for the SOCI Act - one that would not require legislation or regulation - relates to advice regarding 'all hazards' approaches to security. We submit there is scope for more prescriptive guidance as to what constitutes an 'all-hazards' approach, highlighting key areas of security across the four security domains SOCI covers. In PwC's recently published report *After Life: Critical Infrastructure and the e-waste data threat*, we highlighted the significant data and cyber security threats e-waste and its insecure disposal pose to Australian organisations, notably critical infrastructure.[14] We found that the data stored on these devices and their components could contain sensitive PI and system data that, in the hands of malicious actors, could result in significant cyber and data breaches. To this end, more thorough guidance as to the secure disposal of e-waste and other often overlooked threats could be considered as part of the Strategy.

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

At PwC, we work with numerous boards to help directors effectively navigate complex issues and to fulfil their obligations under Section 180 (1) and (2) of the Corporations Act 2001, broadly recognised as 'due care and diligence' and the 'business judgement rule'.[15] Unsurprisingly, cyber security is a key issue for boards and, as highlighted in the Australian Institute of Company Directors' (AICD) most recent Director Sentiment Index, it was the number one issue keeping Australian directors awake at night.[16] Therefore, it can be reasonably inferred that many directors are acutely aware of the risks associated with cyber-related issues and how these risks could impact their obligations as a director. This sentiment was reflected in a 2022 speech by Australian Investment and Securities Commission (ASIC) Chair Joseph Longo, in which he stated: "Cyber risk is very much the new frontier of market integrity … Boards play a key role in recognising and managing risk, including cyber risk. They should consider where they have an obligation to report breaches to ASIC, and where it may be appropriate to make disclosure to the market as either continuous disclosure or in financial reports. This year we see a number of risks emerging that will need to be assessed and managed by directors".

Therefore, while cyber risks should be a key concern for directors, we submit that Section 180 (1) and (2) of the Corporations Act are necessarily broad, and should not be amended to specifically address cyber-related obligations. There are three key reasons we have reached this position:

- Cyber security is a foreseeable and predictable business risk, like many other business risks. Therefore, we believe it should be treated at law like other risks and not specifically carved out as an exception. We submit the potentially broad application of Section 180 in its current form could capture cyber-related director obligations if required.
- It is vital for boards to have 'diversity of thought', composed of directors with a variety of expertise from different professional, cultural and gender backgrounds. While we believe directors should increase their level of cyber knowledge, this should not come at the expense of boardroom diversity - not every director needs to be a cyber expert.
- While cyber security risks are relevant to many industries, singling out cyber risks within Section 180 would act to elevate it above other risks that boards must consider. While this might be appropriate for certain sectors, cyber risk may be a lower order risk for other sectors (e.g construction), but would require all directors, regardless of sector, to prioritise management of cyber risk beyond more pressing business risks.

As it stands, there is a lack of clear guidance related to directors' obligations and cyber security. Therefore, rather than amending the Corporations Act, provision of clearer guidance either by the government or ASIC could be considered as part of the Strategy. Such guidance does not need to be highly prescriptive but could provide clearer steps to support boards in relation to cyber concerns, in a similar vein to that provided by APRA for CPS 234 entities.[17] We note that in 2022, the AICD and the Cyber Security Cooperative Research Centre released better-practice guidance principles in relation to boards and cyber security, which have proved a useful resource to help guide directors.

[13] Critical Infrastructure Information Act | Homeland Security
[14] Critical infrastructure and the e-waste data security threat
[15] CORPORATIONS ACT 2001 - SECT 180 Care and diligence--civil obligation only
[16] Director sentiment falls amid global economic uncertainty | Director Sentiment Index 1H22
[17] Prudential Standard CPS 234 Information Security

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

While PwC does not explicitly oppose legislating a stand-alone Cyber Security Act, we are concerned that such an Act, if not appropriately drafted and implemented, could result in duplication and over complication. This may serve to hinder, not help, cyber uplift across the economy.

The key point that must be considered is: What would be the purpose of such an Act? The Discussion Paper states that the Act would work by "drawing together cyber-specific legislative obligations and standards across industry and government".[18] However, in practice, such a task would be difficult and time consuming. For example, the creation of a single Act, drawing together cyber-related aspects from other legislation, would involve significant overhaul and appropriate amendment to a range of other Acts. Furthermore, the removal of cyber-related aspects of other Acts could, in practice, lead to the interpretation and application of other pieces of legislation being impotent or no longer relevant. To avoid such consequences, other Acts may have to be significantly redrafted before being passed back through the parliament. Not only would such an exercise be costly, it would also take a significant amount of time. We submit that such an investment of time and resources may be better directed at supporting uplift across the economy through alternative mechanisms, for example, education and enhanced guidance.

As previously noted, this is an area in which we believe the new Coordinator could play a key role, acting as a 'clearing house' for cyber-related legislation and regulation in Australia. As stated earlier, there is a clear mandate for the Coordinator to develop a public central repository of all cyber-related legislation and regulation currently in place across the economy, breaking it down sectorally to reduce confusion and ease the burden of compliance duplication. Such an undertaking would help better pinpoint areas for legislative reform and harmonisation and act as a 'single source of truth', ultimately supporting economy-wide cyber uplift.

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?"*

Legal obligations are a critical lever to maintain cyber resilience in the Australian economy. There is opportunity to simplify an increasingly complex patchwork of legal obligations if Australia can move towards a more integrated and streamlined regulatory framework.

Organisations need to navigate complex legislative and industry frameworks such as the Information Security Manual (ISM) for Commonwealth Government-related services and technologies, SOCI Act obligations, Privacy Act requirements for the security of personal information, and Consumer Data Right safeguards for information security. Further rules can apply depending on the nature of the business, such as APRA's CPS 234 for APRA regulated entities, Australian state-specific cybersecurity obligations where business operate within these government supply chains, and international laws for multinational corporations (eg. EU General Data Protection Regulation [GDPR]).

Alignment of legislative frameworks should be prioritised as a means to progress Australia's cybersecurity agenda. As noted throughout this submission, this opportunity must extend to other consultations and inquiries occurring concurrently, like the Privacy Act Review, Digital Platform Services Inquiry, and the Consumer Data Right (CDR) sector-by-sector roll out.

In our experience, a systematic approach to monitoring compliance obligations would include the following steps:

- A mapping of cybersecurity-related obligations that can typically apply to Australian businesses (including legislative issues in the pipeline like digital citizen identity and privacy reforms);
- Analysis of duplication or similar requirements; and
- Development of a plan to harmonise key obligations to simplify compliance management activities.

Once completed and a baseline established, regulatory burden could be mapped over time. Importantly, analysis needs to be agile and also consider current and emerging cyber risks, for example, Australia's complex data retention laws and emerging issues pertaining to artificial intelligence, and to what extent legislative frameworks can govern these risks.

Finally, there may be an opportunity to harmonise underlying guidance and tools that can also vary for each legislative instrument (eg. tools for the reporting of information security incidents), easing regulatory and compliance burden for organisations.

[18] 2023 - 2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER | Home Affairs, P17

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?

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

At PwC, we have worked with numerous organisations impacted by ransomware attacks, aiding incident response and remediation and undertaking post-incident review. In our experience, no two incidents are the same and, given the specific circumstances of an organisation, responses also vary. However, our advice to clients in regard to paying a ransom is always the same: PwC does not recommend paying a ransom unless there is a threat to life. This broadly aligns with the ACSC's view.[19]

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

In our experience assisting clients suffering a ransomware attack, directors will often ask for advice and guidance in relation to the legality of the payment of ransoms and whether payment is a viable option given the legal complexities. In our view, many boards engage in this line of analysis in order to ensure they have appropriately considered payment as an option (and the associated legal risks) to ensure compliance with their obligations under Sections 180 and 181 of the Corporations Act.

Without clear guidance from the government on the legality of ransom payments and how this interacts with the board's obligations under Sections 180 and 181, boards will continue to feel that they need to consider ransom payment as an option by law. Given the government's current position that ransom payments should not be made and the difficulties that the government may face in relation to articulating a clear and decisive position on the legality of ransomware payments under existing legislative regimes (e.g anti-money laundering, proceeds of crime and sanctions regimes), which are inherently complex, the government could consider providing clear guidance on a board's obligations in relation to considering the payment of ransom. If the government was to make it clear that in a ransomware scenario a board is required under sections 180 or 181 not to consider payment, this would allow certainty for boards who wish to take a robust non-payment position.

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

Australia has a key role to play in assisting our regional neighbours build cyber resilience and, to date, has provided significant support to this end. Therefore, we submit the Strategy should ensure appropriate funding is allocated for the continuation of this work and, further, consideration should be given to leveraging PPPs to further enhance cyber resilience and response in the Indo-Pacific.

A key example of this work is the Cyber and Critical Tech Cooperation Program, through which the government has partnered with Indo-Pacific countries to enhance their cyber resilience, including through cooperation on cyber safety, cyber security and cybercrime. This program plays an important role in supporting Australia's international cyber engagement and promoting the United Nations' norms of responsible state behaviour in cyberspace, which aims to foster a free and secure internet that protects national security and promotes international stability, while driving global economic growth and sustainable development.[20] Furthermore, it was highlighted in a recent speech by Assistant Minister for Foreign Affairs, Tim Watts, who noted the key role Australia has played in supporting regional neighbours during cyber attacks. Minister Watts noted that Australian cyber security experts and diplomats had been invited by Pacific countries to help respond to major cyber crises, helping to recover countries' communication systems, payment systems and citizen data after devastating ransomware attacks.[21]

Beyond government, the private sector also has a role to play in building regional cyber resilience. As threat intelligence mechanisms are enhanced domestically, there is the potential to expand such systems to governments and key organisations operating in the Indo-Pacific, ensuring they can better mitigate new threats. And beyond intelligence sharing, there is a key role the private sector can play in supporting knowledge sharing and transfer via mechanisms such as

[19] Ransomware in Australia
[20] Capacity Building | Australia's International Cyber and Critical Tech Engagement
[21] Closing Address to the Australian Strategic Policy Institute's Sydney Dialogue

webinars, online learning programs and staff secondments. Such schemes could be administered by the Department of Foreign Affairs and Trade (DFAT) and could be considered as part of the Strategy.

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

Australia is fortunate to have strong and enduring international partnerships, which are currently leveraged to enhance cyber security posture across these alliances. Most notably, our 'Five Eyes' alliance with the US, UK, Canada and New Zealand - which was built around shared signals intelligence - has been sustained since 1946. Cyber security is a key focus of the Five Eyes, evidenced by joint announcements targeting malicious cyber activity[22] and ongoing collaboration on issues like zero-trust security.[23] However, given the intelligence focus of the Five Eyes and the classified nature of this work, it is difficult to comment as to how or whether this could be enhanced.

The Quad - an alliance comprising Australia, India, Japan and the US - is of particular regional significance and has actively advocated for other nations to abide by global cyberspace norms and the rules-based international order. In 2021, the Quad Senior Cyber Group (QSCG) was established to facilitate regular meetings of expert leaders from across the alliance, working to expand cybersecurity cooperation and strengthen cyber resilience and critical infrastructure protection in the Indo-Pacific. In 2022, members agreed on Joint Principles to guide cyber security cooperation between partners.[24] Stemming from the strong foundations of the Quad, Australia has leveraged a critical technology partnership with India[25] and enhanced strong relations with Japan through a joint declaration on security cooperation and Special Strategic Partnership.[26] Given the regional importance of this work, we submit the Strategy should ensure adequate funding is allocated for continued engagement and collaboration.

Australia's most recent alliance, AUKUS, with the US and UK, is focussed around defence technologies and, we submit, offers significant opportunities for the development and sharing of advanced cyber technologies and intelligence. However, for this to occur effectively, action is required in several key areas, which were highlighted in our recent report *Maximising Australia's AUKUS Opportunity*, which we submit should be addressed as part of the Strategy. These include:

- Existing migration policies, which need to be enhanced to support an AUKUS workforce, and issues surrounding joint recognition of security clearances across nations;
- US export control laws, which currently disincentivise cross-border research and development;
- Defence cultural change and increasing risk appetite; and
- The need for innovation in defence procurement practices.[27]

Finally, it is worth noting Australia's leadership in the establishment of the International Counter Ransomware Task Force (ICTRF), of which Australia is chair. Via the ICTRF there is a significant opportunity to work with the global alliance of more than 30 countries to tackle the ransomware ecosystem through threat intelligence sharing and the development of best practice guidance for countering ransomware. We submit that leveraging PPPs could serve to enhance the outcomes of the ICTRF and provide insights and perspectives that could support its objectives.[28]

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

In our experience cyber security in government can be siloed across various departments and agencies. The Cyber Hubs pilot, which is ongoing, has served to break down some of the existing barriers and encourage other departments and agencies that fall under the hubs to take more integrative and collaborative approaches to cyber uplift. However, more needs to be done.

Government institutions have consistently failed to reach cyber maturity goals, with the most recent *Commonwealth Cyber Security Posture Report* finding almost 90% of Australian government entities are not implementing basic cyber resilience

[22] Five Eyes warn about hacking dangers in wake of China cyber attacks
[23] Five Eyes alliance meets to discuss zero-trust cyber security
[24] Quad Senior Cyber Group
[25] Australia-India Cyber and Critical Technology Partnership (AICCTP)
[26] Australia-Japan Joint Declaration on Security Cooperation | Australian Government Department of Foreign Affairs and Trade
[27] MAXIMISING AUSTRALIA'S AUKUS OPPORTUNITY
[28] Cyber security - Counter Ransomware Initiative

protections.[29] Furthermore, a 2021 report by the Australian National Audit Office (ANAO), which analysed nine non-corporate government entities, found the implementation of cyber security risk mitigation strategies was not fully effective.[30] Therefore, we submit that given the expectations government has on the private sector to enhance cyber posture, there is clear scope for government to improve its cyber posture and lead by example.

We understand that government cannot do this alone and believe there is a key role for PPPs to play in this space via mechanisms like enhanced threat sharing, knowledge transfer opportunities and greater collaboration. This Strategy provides a significant opportunity not only for the government to illustrate leadership but to model a collaborative approach by working more closely with industry.

We also believe there is an opportunity for government to share more success stories around efforts where cyber security has been an enabler of trust for the digital services that citizens rely upon. A recent example of this is the 2021 Digital Census which was delivered seamlessly and securely to millions of Australians. Sharing these stories, and details of how good cyber security was practised, will serve to encourage a more open dialogue across government and industry and allow for lessons learned to be quickly applied and replicated.

Another key lever is government procurement practices and the setting of minimum cyber standards for vendors, which is explored below.

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

As previously noted, the CTIS program is currently the main government-led mechanism for cyber threat intelligence sharing. The other key mechanism facilitated via the CISC for critical infrastructure entities is the Trusted Information Sharing Network (TISN). While the cross-sectoral TISN serves several purposes, members can benefit from up-to-date government and industry information on threats and hazards, post-incident lessons and best practice guidance on security and resilience.[31]

While we support moves to enhance government and industry threat intelligence sharing, we believe that the CTIS program needs to be reviewed. In our opinion, there are several key issues with the program that need to be addressed:

- The benchmark for organisations to participate in the program is high. For example, organisations must have threat intelligence and engineering capacity to make full use of the CTIS. This makes it difficult for SMEs to access.
- CTIS is not 'plug and play' - the platform is overly complex and involves dedicated learning for proper utilisation.
- The system does not have appropriate mechanisms in place to encourage information sharing and to ensure that information shared is not misused.
- While 28,000 IOCs have been reported, in reality this figure is low and does not represent an accurate illustration of the Australian cyber threat environment.

Furthermore, a cultural shift within ASD and ACSC is required to facilitate better threat intelligence sharing. While progress has been made, barriers remain in terms of opening up lines of communication with industry and working with industry, which is impacted by intelligence classification levels even when a threat has been detected at an industry level. In our view, when it comes to threat intelligence sharing, the more aggregated data available the better the outcome, and industry monitoring provides a lot of data that could serve to enhance threat intelligence sharing and threat response mechanisms. We submit there is scope for the Strategy to consider how the current intelligence classification system operates and whether it should be downgraded in the event industry has knowledge of a specific threat and relevant information to share.

A clear example of the divide that persists in relation to government-industry cyber collaboration is the failure of the Joint Cyber Security Centres (JCSCs) to foster meaningful industry engagement. With new ASD/ACSC offices launching in Melbourne and Brisbane, we submit there is a clear opportunity to build collaborative engagement initiatives and work better together. A model that could be leveraged to support and grow such an approach is the UK's Industry 100 program, which is outlined below.

[29] Basics baffling govt agencies after 'cyber slumber'
[30] Cyber Security Strategies of Non-Corporate Commonwealth Entities | Australian National Audit Office (ANAO)
[31] https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/tisn-overview.pdf

UK - Industry 100
Industry 100 (i100) is a key initiative led by the UK's National Cyber Security Centre (NCSC) to facilitate close collaboration with the cyber industry. i100 brings together public and private sector talent to work together to solve complex cyber challenges, promoting innovation, driving collaboration and enhancing a shared understanding of cyber security, from NCSC and industry perspectives. i100 secondees from industry work across a wide range of placements on a part time basis, ranging from one day a week to one day a month. Participating organisations continue to pay the salary of their staff member while on secondment with the NCSC to maintain independence.[32]

In developing enhanced threat intelligence sharing models for the Strategy, there are several successful international examples upon which an Australian approach could be modelled. At the heart of these models is a strong focus on PPPs and how working with industry can enhance domestic cyber threat protections. These are summarised below.

US: National Security Agency - Cybersecurity Collaboration Centre
The National Security Agency's (NSA) Cybersecurity Collaboration Center (CCC) leverages the strength of industry partnerships to mitigate and respond to foreign cyber threats to National Security Systems (NSS), the Department of Defense (DoD), and the Defense Industrial Base (DIB). Operating upon three key principles - Detect, Innovate and Mitigate - the CCC has fostered an environment for information sharing between NSA and its partners, combining specialised expertise to help develop a whole-of-nation approach to cybersecurity.[33] Through the CCC's Fusion Operations, analysts and prototypers work hand-in-glove with industry, academia, and government to understand gaps, seek signals intelligence seed values, and provide analysis using unclassified resources to solve shared analytic and development challenges.[34]

UK: Cyber Security Information Sharing Partnership
The Cyber Security Information Sharing Partnership (CISP) is a joint industry and government digital service to allow UK organisations to share cyber threat information in a secure and confidential environment. A new and enhanced CISP platform is currently under development.[35] Highlighting the importance of strengthening PPPs in the UK context, the first pillar of the National Cyber Security Strategy 2022 is: "Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry".[36]

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?

PwC would be supportive of the introduction of an explicit obligation of confidentiality by the ASD and ACSC in relation to interactions with organisations experiencing a cyber incident. This would support more open and frank information sharing by impacted organisations, which would ultimately support stronger response mechanisms. However, such confidentiality should not serve to obfuscate the responsibilities of impacted organisations in fulfilling their regulatory obligations in relation to reporting cyber incidents if such reporting is required.

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?

While there are valid reasons to expand existing regimes for the notification of cyber security incidents, we submit that public education should not be a key driver. However, such a move would support improved visibility as to the size and scale of cyber incidents and help identify key trends and threat vectors. Organisations could leverage such information to mitigate cyber threats.

In terms of improving public understanding of the nature and scale of ransomware and extortion, we submit that focussed public education and engagement campaigns are required. Again, in this space, there is a key role for PPPs to play, as

[32] About - NCSC.GOV.UK
[33] About - Cybersecurity Collaboration Center - Overview
[34] About - Cybersecurity Collaboration Center - Fusion Operations
[35] CISP - Cyber Security Information Sharing Partnership - NCSC.GOV.UK
[36] National Cyber Strategy 2022

many organisations, including our own, have expertise in the effective delivery of cyber security education programs for a range of diverse stakeholders. Working with the government, there is an opportunity to leverage industry networks and expertise to act as a multiplier.

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

Australia has a significant cyber skills gap, a problem which has been acknowledged by the government and industry alike. This is not a problem confined to Australia, however, as our reliance on digital systems continues to grow, it is an issue that needs to be dealt with now to mitigate further shortages into the future. Furthermore, when considering the cyber jobs that need to be filled now and those that will need to be filled in the future, skills transferability and uplift will need to be a focus, given some of the jobs of today will be automated in the future. For example, as artificial intelligence (AI) and machine learning (ML) become more ingrained in organisational processes, the need for cyber analysts may reduce. And while this will not happen overnight, given the fast-moving pace of the cyber space, continuing professional development and upskilling will be vital.

While there is a key role for the government to play in tackling the skills gap, the government alone cannot solve this problem and we submit there is a key role for PPPs to play in creating a skilled cyber workforce for Australia. For example, at PwC, we offer a Higher Apprenticeship Program, which provides an alternative career pathway for those not wishing to attend university. Participants have the opportunity to obtain two VET (Vocational education and training) qualifications in Information Technology (IT), earning the Certificate IV followed by a Diploma. Once completed, participants have the chance to join PwC's Graduate program.

Education

A key barrier to entering the cyber workforce is the general requirement to hold a relevant tertiary-level qualification or degree. Currently, many entry-level jobs require such qualifications, which may prevent many interested citizens from pursuing a career in cyber security, especially those looking to reskill. For many Australians, there are significant barriers to attending university, including familial and employment commitments, as well as financial barriers.

Several programs are in place to help address this issue, like the Federal Government's Digital Traineeship and Digital Apprenticeship programs.[37] However, as with many of the challenges raised in the Discussion Paper, PPPs will play a key role in driving successful outcomes. To this end, the Federal Government has already announced support for a Digital and Tech Skills compact between government, unions and technology employers,[38] which is a step in the right direction. The compact, which is aimed at delivering industry-based digital apprenticeships, will be crucial to filling the growing cyber skills gap, providing a viable pathway for more Australians to gain cyber security education and enter the cyber workforce.[39]

Immigration

PwC supports steps by the government to help build Australia's cyber workforce through migration policies that serve to attract skilled cyber professionals from abroad. As noted by the Tech Council of Australia (TCA), migration must play an important role in providing highly specialised and experienced tech workers which equates to about 43,000 additional skilled migrants required on top of a forecast 119,000 under a business-as-usual scenario.[40] These skilled migrants have much to offer in terms of experience and mentorship and can help train today's graduates for the challenges of the future. Such support is invaluable in building and strengthening the pipeline of homegrown cyber talent and serving to highlight the myriad of opportunities the cyber industry presents. Furthermore, the Grattan Institute has observed that, "a less prescriptive (migration) system that helps attract the world's best and brightest is key to strengthening our sovereign capabilities in areas like cyber security".[41] We submit that enhanced resourcing to support visa processing times in Australia would support organisations in recruiting more international cyber professionals to work in Australia.

Accreditation

Australia currently has no official accreditation program for cyber security professionals, which means people with the skills but without the appropriate tertiary qualifications are often cut out of the jobs market. Therefore, we submit a key mechanism to get more cyber professionals into the workforce would be the establishment of an official, government-mandated cyber security professional accreditation program and administrative body.

---

[37] Emerging talent programs
[38] Digital and Tech Skills Compact
[39] Digital Apprenticeship Program
[40] Getting to 1.2 million, P6
[41] How rethinking skilled migration can solve some of our biggest problems | Grattan Institute

A central component of such a program would be the implementation of competency-based accreditation. This would remove the need for tertiary cyber education and support self-taught and on-the-job learners to receive official accreditation for their skills. It would also support skilled migration, providing a pathway for skilled migrants with cyber skills to gain accreditation without the need for further education.

Essential to the program would be the establishment of an independent accreditation body, that would oversee the conferral of accreditations. We submit that such a body could be modelled on existing professional accreditation bodies

We live in a digital world and geography should not present a barrier to accreditation. Therefore, we believe online delivery of accreditation competency modules would best support the program. It would enable cyber professionals from Adelaide to Alice Springs to gain accreditation without leaving the house. Furthermore, an online platform would streamline the process, getting more cyber professionals into the workforce more quickly.

13. 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?*

PwC is supportive of the establishment of a single cyber incident reporting portal, which would reduce administrative burden during a cyber incident, with administration of such a portal the responsibility of the Coordinator.

Currently, organisations with similar but slightly differing cyber notification obligations for a number of regulators, under a number of regimes, are required to make numerous notifications in the event of an incident. For example, some APRA-regulated entities are required to make notifications under the SOCI Act, the Privacy Act and prudential standard notification obligations. In our experience, this duplication causes significant administrative burden when an organisation is in the midst of a cyber incident.

As a result of multiple regimes operating across different jurisdictions and sectors, there are varying levels of incidents requiring notification, unnecessary duplication of notifications and differences in timing and information needs, as well as the risk of missing a required notification. Harmonisation of notifiable requirements would increase efficiency and simplify the notification process, both for entities and government, and ensure incident response, not regulatory response, is the foremost priority for impacted organisations.

We note that as part of an integrated reporting portal, consideration would need to be given as to how to manage different details to be shared with different regulators, how data may be shared among regulatory bodies and whether there are data breach notifications under the CDR requiring alignment. Further, we submit accessibility should be limited to specific regulators as determined by the notifying organisation.

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

Central to government-led effective post-incident review and consequence management is the coordination of such activities through a single channel. Such activities should be led by the Coordinator, noting that in the recent job advertisement for the role key responsibilities included leading coordination across government and industry to manage any consequences of cyber incidents across the economy, and driving lessons learned into policy development to continuously improve Australia's cyber resilience.[42]

In undertaking post-incident review, a certain level of privilege should apply to help ensure organisations are transparent and frank with government in relation to an incident. If a certain level of privilege is not given, organisations may be hesitant to speak openly or make full disclosures. However, such a process should be of benefit to the broader economy. Therefore, we submit that the public release of high-level recommendations should be allowed to help better protect other organisations against cyber threats and to highlight root causes (if possible), which would serve to help strengthen specific cyber security outcomes across the economy. At PwC we observed such a trend in the wake of recent data breaches, when many organisations sought to ensure their API security was adequate and that their data collection, retention and disposal practices were compliant.

[42] National Cyber Security Coordinator

We note that after the recent data breaches, a review of the government's response by CEO of the Cyber Security Cooperative Research Centre, Rachael Falk, was undertaken (the Falk Review). The Falk Review has not been publicly released and, while it is understandable the whole report cannot be released, it would be useful for industry to be provided with a high-level view of the Falk Review's findings and recommendations. This would also serve to assist organisations better understand what information and access the government may require in the event of a significant breach, and develop incident response plans accordingly.

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?*

As previously noted, there is a key opportunity for government to lead multi-channel tailored education and public awareness campaigns to help improve public knowledge of cyber security and cyber threats. Such campaigns should capture all demographics, from children to seniors, and account for the diverse cultural and linguistic composition of the Australian community. Through hardening of government systems there is also a significant opportunity to better protect Australians, simply by making online services safer for those who interact with them.

Industry can - and does - come to the table by offering customers cyber-related education and information as part of service delivery. The financial services sector provides an excellent example of this type of work, which ranges from the provision of timely threat warnings through to operational changes to support security, for example, by only communicating with customers through apps to reduce the rate of phishing and email compromise. These are not complex solutions but they are extremely practical, ultimately helping better protect Australians when they are online.

While consequence management in the wake of a cyber incident varies given the nature of the incident and whether personal information was compromised, there are key levers that can be pulled to better protect those impacted. For example, reimbursement for the replacement of official identification documents compromised in a breach is a practical way organisations can support victims, as is the provision of credit monitoring services to detect financial anomalies. Given the often 'long tail' of cyber incidents, such mechanisms may need to be implemented for a longer period of time, which could be mandated by the Coordinator on a case-by-case basis.

SME cyber security

When it comes to cyber uplift, SMEs often struggle - they are time and resource poor and, in terms of business operations, cyber security is not always a primary concern. Furthermore, cyber uplift can be expensive and, in a tough economic environment, spending money on cyber uplift may not be a high priority. But there are things that can be done.

From a government perspective, SME incentivisation could play a key role. For example, the government could more effectively promote the use of taxation mechanisms like instant asset write-offs, to encourage more SMEs to invest in cyber security. Given the Privacy Act's small business exemption could be scrapped as part of ongoing reforms, this is an area that requires more attention, given the number of organisations captured would increase significantly with significant consequences for the cyber security requirements of SMEs right across the economy. At the heart of the Privacy Act is the need to protect PI which, in a connected world, means ensuring effective cyber security protections are implemented. For SMEs, this has the potential to present both regulatory and resourcing burdens, which must be considered in lock-step with the Strategy. Therefore, we submit that there is an opportunity via the Strategy to better educate SMEs about cyber security through direct engagement, prescriptive guidance and incentivisation measures.

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?

While Australia's cyber-related research system is world class, in our view this excellence has not translated into large-scale successful commercial outcomes. As noted in the *University Research Commercialisation Action Plan*, released February 2022: "This limits the economic impact of our universities and shrinks the return on investment from publicly funded research. Too often, research that could be used to benefit our economy and communities is not taken through to

innovations which can create new products and services, create jobs and lift productivity in businesses".[43] This trend was further highlighted by Australia's Chief Scientist Dr Cathy Foley in a recent speech, in which she noted Australia's failure to commercialise domestic innovations like the Black Box and solar panels occurred because "we did not take this research seriously enough or have the confidence and capability to commercialise it".[44]

If Australia is to fully embrace the opportunities offered by the development of cyber-related technologies, this is a trend that needs to change. Therefore, we submit that a thorough analysis of the successes and failures of previous and ongoing cyber-related research and development funding could be undertaken so a strategic approach to research and commercialisation funding can be developed. Furthermore, PPPs can play a vital role in driving such innovation, with industry identifying problems requiring new solutions, helping guide highly focused and practical research and development programs. While we note the Cooperative Research Centres (CRC) and Cooperative Research Centres Projects (CRC-P) programs go some way to achieving this objective, the current system is not agile enough to deal with new and emerging problems and the dynamism of the cyber landscape. A potential solution could be the provision of greater flexibility within the CRC and CRC-P systems, facilitating the agility to address new and emerging challenges without the need to undertake onerous contractual variations.

A current, and highly relevant, example are quantum technologies, in which Australia's domestic capabilities are considered world class. Recently UNSW made a breakthrough in delivering the world's first integrated circuit at the atomic scale[45] and a number of Australian start-up companies, including Quintessence Labs and Quantum Brilliance, are taking products into the mainstream market. In the past year, we have started to advise many organisations on the future benefits and risks of quantum computing and quantum cryptography, demonstrating there is interest in and growing demand for these technologies and commercial opportunities across the private and public sectors. This presents a clear area in which Australia can excel, leveraging the sovereign capability we already have to drive a world-leading cyber capability.

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?

Government procurement could be used as a powerful tool to uplift Australia's cyber security ecosystem and promote homegrown cyber-related innovation. There are two key mechanisms we believe would help drive a procurement-based agenda:

- Minimum cyber security standards could be mandated for organisations feeding into the government supply chain;
- The introduction of 'innovation procurement' policies.

Minimum cyber security standards

By establishing minimum cyber security baselines for organisations feeding into government supply chains, more organisations would be incentivised to improve their cyber posture to ensure eligibility for government tenders. Given the government's huge procurement spend, which in FY 2021-22 comprised 92,303 contracts with a combined value of $80.8 billion, there is a clear opportunity for government to set a cyber-uplift agenda.[46]

The transformative role such a shift could entail was highlighted by Rajiv Shah in his 2020 report *Working smarter, not harder*, which notes: "Setting security standards expected from its (government's) suppliers may help to lift standards across the board. Companies will be incentivised to lift their standards in order to qualify to do business with the government, and it will often be easier for them to apply those standards across their whole enterprises rather than just for their government contracts".[47] There is also an opportunity to highlight the importance of cyber security in the Commonwealth Procurement Rules, noting that currently, it is mentioned just once.[48]

[43] University Research Commercialisation Action Plan, P8
[44] Dr Cathy Foley Delivers the Thomas Baker Oration 2022
[45] UNSW quantum scientists deliver world's first integrated circuit at the atomic scale
[46] Statistics on Australian Government Procurement Contracts | Department of Finance
[47] Working smarter, not harder | Australian Strategic Policy Institute | ASPI
[48] CPRs - 1 July 2022

Software Bill of Materials

In the US, the establishment of minimum software standards is serving as a procurement lever to bolster cyber security. In 2021, the Department of Commerce and the National Telecommunications and Information Administration published the "minimum elements" for a Software Bill of Materials (SBOM), following an Executive Order on Improving the Nation's Cybersecurity by President Joe Biden.[49] An SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which produces multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks. In 2022, a Memorandum for the Heads of the Executive Departments and Agencies was released, mandating that: "Federal agencies must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices". Furthermore, "a SBOMs may be required by the agency in solicitation requirements, based on the criticality of the software" and "Artifacts other than the SBOM (e.g., from the use of automated tools and processes which validate the integrity of the source code and check for known or potential vulnerabilities) may be required if the agency determines them necessary".[50] Ultimately, this means to be procured by US Government departments and agencies, software providers have to meet minimum security standards and, if asked, provide technical information like source codes.

Innovation procurement

In relation to fostering sovereign cyber innovation, we submit that the establishment of a national 'innovation procurement' model, driven by public investment, could be considered.

The European Commission defines innovation procurement as:

- the development of innovative solutions through the procurement of research and development services
- the procurement of innovative solutions that are not yet available or do not exist on the market
- the procurement of innovative solutions that do exist but are not yet widely available on the market.[51]

Innovation procurement can help shape and create new markets; drive economic growth; drive increased uptake of innovative products and services; and support new businesses' access to the market, particularly small and medium businesses.[52] A recent report from Flinders University's Australian Industrial Transformation Institute found that, beyond industrial growth, innovation procurement "serves nations' interests in achieving a degree of sovereign capability and self-sufficiency in the face of external shocks, and defence challenges. Increasingly, innovation procurement is also targeting benefits of environmental sustainability, liveable cities, decarbonisation and inclusive growth".[53]

Renowned as an innovation leader and the 'start-up nation', Israel provides a useful case study in the successful application of innovation procurement for the development of critical technologies. The Israel Innovation Authority (the Authority) is an independent publicly-funded agency that provides tools and funding platforms to drive progress right across the innovation ecosystem. This includes early-stage entrepreneurs, mature companies developing new products or processes, academia, global corporations interested in collaborating with Israeli technology, Israeli companies seeking new markets abroad and traditional factories and plants seeking to incorporate innovative and advanced manufacturing into their businesses.[54] It comprises six divisions – start-up, growth, technological infrastructure, international collaboration, advanced manufacturing and societal challenges – each offering customised and comprehensive incentive programs.[55] The Authority builds on other Israeli Government initiatives like the Yozma program, which kick-started the nation's thriving venture capitalism ecosystem.[56]

[49] The Minimum Elements For a Software Bill of Materials (SBOM)
[50] September 14, 2022 M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
[51] Innovation procurement
[52] Ibid 51
[53] Innovation Procurement Lessons For Australia
[54] The Israel Innovation Authority
[55] Ibid 54
[56] Overview - Yozma

The CHIPS and Science Act

On 9 August 2022, the US Congress passed the CHIPS and Science Act. The Act provides US$280 billion (A$410.6 billion) funding to build a domestic semiconductor industry, representing the largest investment in research and development in US history.[57] The shoring up of a domestic US semiconductor industry is a critical national security priority, with semiconductors the single most important technology underpinning leading-edge industries. Semiconductors are essential for the effective operation of 'everything from smartphones to nuclear submarines and from medical equipment to wireless communications'.[58] While we understand this type of investment is not appropriate in the domestic context, it does indicate that research and industry and development programs focused on solving specific problems are gaining momentum. Furthermore, from an Australian perspective, creative thinking can help leverage international programs like the Act. For example, the Act presents significant opportunities for Australia and the AUKUS agreement more broadly. Australia has significant reserves of high-quality critical and rare earth minerals, which can provide the raw materials required for semiconductor production. These reserves offer significant economic and strategic opportunities, with the potential to support alliance supply chains and enhance Australia's sovereign capability.[59]

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

Across the innovation spectrum, new and exciting technologies are being developed everyday and, for many of these technologies, their operations rely on internet connectivity. Therefore, as the Internet of Things (IoT) continues to grow at an exponential rate, cyber security needs to be a key consideration and security- by-design principles adopted. Furthermore, a number of new and emerging technologies have the potential to support cyber uplift but also produce new threat vectors. Two key technologies in this space are quantum computing and AI ,which we explore in this submission.

Quantum computing

Quantum technologies have the potential to be transformative. They will impact the way we do business, secure our data and help solve some of the most complex problems facing humankind. Breakthroughs are being made every day and Australian quantum technologists and academics are punching above their weight in the quantum race. But quantum is a concept that can be hard to grasp and, while the diverse variety of quantum technologies offer much potential, they also present risks, notably in relation to cyber security. This is not a distant threat - quantum-safe cryptography is an active field today and organisations need to take a proactive approach in understanding and mitigating these risks. Given Australia's vibrant quantum industry, the Strategy offers an opportunity to work more closely with sovereign talent to enhance our nation's quantum capabilities now and into the future.

In terms of enhancing cyber security, quantum technologies promise to add efficiencies and introduce greater protections. Some of the opportunities quantum technologies of the future present include:

- Augmentation of AI and ML, processing and spotting data patterns rapidly (including in relation to cyber monitoring), leading to more accurate and scalable quantum AI/ML tools
- Quantum cryptography and application for stronger security and key management, such as Quantum Key Distribution (QKD)
- Solving optimisation problems that currently require complex modelling and simulations.

However, there are also risks to security associated with quantum technologies. For example:

- Quantum decryption capabilities could put most current encrypted communications infrastructure at risk of exploitation (post-quantum cryptography)
- Ethical and integrity challenges associated with outcomes of quantum computation and quantum-enabled AI
- The World Economic Forum (WEF) has identified possible adverse outcomes of quantum on individuals, business, ecosystems and economies as one of its key technological risks.[60]

While encryption-breaking quantum capabilities are not yet a reality, there are steps organisations can take now to better 'quantum proof' their systems. For example, QKD provides a secure way of sharing encryption keys using the properties of quantum mechanics and is designed to thwart any 'eavesdropping' attempt, essentially destroying the information the attacker was attempting to steal. QKD is proven to be information-theoretic secure, meaning the protocol cannot be broken even by an adversary with unlimited processing power. Put simply, QKD prevents data being compromised by even the most

[57] Explainer: The CHIPS and Science Act 2022
[58] Australia's semiconductor national moonshot | Australian Strategic Policy Institute | ASPI
[59] Ibid 27
[60] The Global Risks Report 2022

motivated adversary and is a technology that should be considered to help protect systems to prevent the harvesting of encrypted data now and decryption in the future.

Artificial Intelligence

AI is currently evolving faster than at any moment before in history. The potential business applications and commercial opportunities for modern AI are significant, however, the costs of moving too quickly without the right safeguards in place are wide-ranging. The risks currently being faced by Australian organisations include inaccurate outcomes and misinformed decisions, selection bias issues, potential operational impacts and disruption, adversarial attacks to manipulate algorithms, and loss of confidential data and intellectual property rights. While significant work has been done examining the ethics of AI and its appropriate applications, we submit the Strategy should continue to build on this work through research and development funding and AI pilot programs.

Generative AI and cyber security

Generative AI is currently making headlines due to the public release of platforms like ChatGPT. And, while generative AI can support cyber uplift by creating software code and help solve human resource shortages across many industries, it also presents new threat vectors. For example, generative AI tools could be used to produce more authentic-looking phishing emails. Furthermore, these tools and their ability to create code also means they can produce malicious code, which could be used by threat actors to create cyber weapons like viruses, worms, Trojans, ransomware and wipers.

Keeping pace with emerging technologies

Through our work we have observed many instances where businesses and governments reactively seek ways to evolve policies and regulations to respond to emerging risks. In order to keep pace, the Strategy, and its associated missions and initiatives, should consider the following:

- Pro-Innovation - The Strategy needs to strike the right balance to mitigate cyber security risks and still realise the opportunity and innovation new technologies represent. For example, the recent growth in accessibility and capability of AI has triggered a wave of reinvention and innovation across virtually every industry, and demonstrates the economy-wide opportunity that emerging technologies can enable. And innovation in digital identity services can drastically improve user experience and productivity across the community.
- Flexibility - The Strategy will need to be flexible to respond to emerging issues. Generative AI is now a key example of how quickly technologies and associated issues can evolve. The Strategy needs to cater for horizon scanning and enable the government to quickly respond to emerging issues (such as education, guidance, advice and other tools) for the benefit of the Australian community.

Security-by-Design is fundamental

The Strategy represents an opportunity to invest in upskilling and capabilities to drive security-by-design practices. In our experience, this core building block of technology is inconsistently applied and is not commensurate with the cyber security risks associated with new technologies. We believe this is a priority area to facilitate fast-paced, secure and trusted digital transformation across the economy and needs to be 'baked in' to tech development.

To this end, there are synergies and learnings associated with related regulatory frameworks that should be explored. For example, the *Privacy Act Review Report* proposes mandatory Privacy Impact Assessments for activities with high privacy risks, and the Consumer Data Right sets out an accreditation process to measure security controls at onboarding of new data recipients. We also submit that previous work undertaken by government in relation to the development of a voluntary cyber security 'star rating' system for new IoT devices could be revisited, and the IoT Code of Practice also reviewed.[61]

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

We agree there is value in measuring national cyber resilience, however, suitable metrics will need to be designed in accordance with the Strategy and its intended outcomes. Furthermore, such reporting, where appropriate, should be made publicly available to help guide the private sector's practices and highlight where improvement is required.

In our experience, quantitative metrics would relate to key areas noted in this submission including:

- Reported incidents

[61] Code of Practice, Securing the Internet of Things for Consumers

- PPP development
- Government cyber uplift
- Procurement practices
- The number of cyber professionals and roles
- Skilled cyber migrant intake
- Skilled workforce pipeline
- Domestic cyber security industry growth
- Community awareness and education programs

Such an approach could leverage existing reporting and measurement practices in the Australian economy, like the ACSC's Commonwealth Cyber Security Posture report,[62] notifiable data breach reports published by the OAIC, and the AESCSF maturity assessment program.

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

In addition to the metrics mentioned above, ongoing evaluation will be important to ensure the implementation of the Strategy meets its intended outcomes and remains fit-for-purpose.

In our experience, holistic cybersecurity uplift strategies can be complex programmes that span a multi-year period and often comprise a broad set of initiatives. Furthermore, these programmes can go off-track without appropriate governance mechanisms.

In the design and implementation of evaluation measures, the following guiding principles should be considered:

- Measurement of outcomes - In a period of economic uncertainty, the reasons for investment and value-for-money will need to be front of mind and demonstrate how this Strategy will result in a net benefit for our community. Use of metrics will be critical to measuring the effectiveness of the Strategy, and can flag where adjustments are required (e.g. scorecard, traffic light indicators).
- Regular review of priorities - Strategic priorities and initiatives should be revisited periodically to ensure goals are aligned with changing needs of the community and an evolving threat landscape. Importantly, this will also need to address areas that are not considered a priority.
- Transparent communications - Clear and transparent messaging can positively contribute to ongoing buy-in as the Strategy is mobilised and implemented. Communications may need to be adjusted for the audience, with this Strategy likely to impact a diverse mix of stakeholders across businesses, government agencies, and community groups.

We also submit that public annual progress reporting (in non-classified areas) would be an appropriate mechanism to illustrate where gains have been made and improvement is required, implementing a simple traffic-light system for ease of comprehension. Furthermore, given the Strategy will span seven years, annual 'mini consultations' may be appropriate to ensure that in the fast-moving and dynamic cyber space, its aims and principles remain fit-for-purpose.

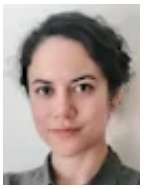
[62] The Commonwealth Cyber Security Posture in 2022 | Cyber.gov.au

Contacts

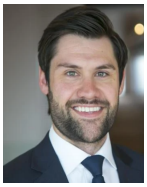
Robert Di Pietro
Partner, Cyber Security & Digital Trust
[redacted]

Anne-Louise Brown
Chief of Staff, Federal Government Cybersecurity and Digital Trust
[redacted]

Natalie Mu
Director, Cyber Security & Digital Trust
[redacted]



Victoria Young
Director, Cyber Security and Digital Trust
[redacted]



James Patto
Director, Legal
[redacted]