COMMENT ON AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

Introduction

CI-ISAC thanks the Minister for Home Affairs and Minister for Cyber Security for the opportunity to provide input into the Cyber Security Strategy 2023-30. CI-ISAC recognises the importance of this capstone document, and as a purpose-driven, not-for-profit Australian business with the mission of increasing the cyber security of Australia's Critical Infrastructure (CI) owners and operators, we take this opportunity to comment on the Cyber Reference Group's Discussion Paper seriously.

Our response will consist of two parts. The first part offers general observations and comments on the Discussion Paper and the challenges presented within the document. The second part comprises answers to those questions on which CI-ISAC is qualified to comment.

The CI-ISAC Board and Advisory Group has prepared this response – a mission-focused group of Australians with extensive experience working in the cyber and national security sectors.

PART 1

Want a better outcome? Change what we are doing.

Lifting and sustaining cyber resilience and security must be an integrated whole-of-nation endeavour. However, the need for a coordinated and concerted effort by governments, individuals, and businesses of all sizes cannot be achieved by doing the same things the nation has been doing. For a start, *greater involvement of local government is vital*, especially for cyber uplift of critical infrastructure. Government and Industry are operators of critical infrastructure, so local government needs to be treated as a sector, allowing better alignment of standards, accountability, and consequence management, and thereby providing critical infrastructure as a service across the public and private sectors. Equally, greater attention needs to be paid to *uplifting the smaller businesses, especially those involved in delivering critical services.* This can be achieved by collective support (central and network capabilities) and the provision of 'turn key' capabilities to accelerate their cyber maturity uplifts.

Support for innovative businesses

For Australians to engage with cyberspace with confidence and assurance, Governments at all levels will need to do more to encourage innovative sovereign businesses through effective implementation plans for supporting digital transformation and improving collective cyber

defence. Cyber-secure technologies for use by Australians, a secure and safe critical infrastructure sector, and better-tailored support for improving the cyber resilience of businesses demand more from Government than policy and regulation (this is expanded below).

Domestic v International focus

The discussion paper is right to note that the Strategy needs to have both a domestic and international focus. The challenge is getting the balance right. While the most harmful cyber threats are usually generated abroad – requiring international cooperation to combat them – the effects are felt locally. The Department of Home Affairs and the Department of Foreign Affairs and Trade will need to work hard on synchronising, balancing and prioritising their respective efforts in addressing domestic and international elements. And they will need to do this while managing a range of concurrent challenges (Note: A National Security Strategy would help with this prioritisation – see below). There is a danger that two parallel efforts will emerge and distract from one another. International partnerships are vital, and Australia needs to be among the leaders in setting and agreeing on international standards; however, Australians rightly expect their domestic interests to be given priority, and CI-ISAC recommends this. The Strategy should emphasise raising the cyber security of public and private networks, servers, operational technologies (OT) resident in Australia, and the protection of Australians' data that reside in these systems. With that said, CI-ISAC notes the intention to include both international and domestic elements in the new strategy.

Clear obligations + simple regulatory framework

The Strategy needs to make crystal clear the obligations Government, businesses and citizens have to help defend Australia's cyber frontiers. The obligations of businesses and government agencies in particular must be clear and transparent – especially when these obligations are legislated. At the same time, the Strategy should aim to minimise the associated regulatory frameworks so these are not an impediment to entities achieving cyber security best practices. Reporting obligations and response requirements following a major cyber incident need to be streamlined. We anticipate that the new National Cyber Security Coordinator will be empowered to work with regulators to ensure an easy-to-implement regulatory framework is established.

While the Strategy needs to deliver best practice standards, evaluation, transparency, reporting, and aligned incentives, together with the appropriate support, accountability and leadership for individual government departments and agencies to manage their cyber security risk profile; the same needs to be provided to businesses both large and small.

This last point leads to the need for better national frameworks to protect against, and respond to, serious cyber attacks and how to support entities to move towards a proactive cyber

defence posture. Improvements across the nation are also needed in terms of cyber threat intelligence sharing and building and skilling Australia's cyber workforce.

We need a National Security Strategy

While the Discussion Paper is silent on this topic, we believe the Government's *Cyber Security Strategy 2023-30 should be nested within a whole-of-nation, National Security Strategy*. The Rudd Labor Government took on this challenge delivering the nation's first, and only, National Security Strategy in 2008. The actors that threaten Australia's 'cyber agency' – hacktivists to criminal groups to nation states - are an immutable feature of Australia's national security landscape, and to consider the cyber domain in isolation, while urgent and necessary, runs the risk of missing elements of national power that can be brought to bear to protect Australia's use of the cyber commons.

Managing Interdependencies. The range of other important Government priorities that will significantly enhance Australia's digital security and progress in parallel with the Strategy highlights the degree of interdependence that describes the overall national challenge. Managing inter-dependencies demands a new approach that starts with a common national vision, common mission, acknowledgement of shared accountability for results, and the need to manage shared risk. Some models such as the Viable Governance Model and Viable System Model act as a blueprint for designing the control and communication aspects of organisations, which can be extended to national government.

Policy and regulation are not golden bullets. These models highlight five main functions or systems: Policy, Intelligence, Control, Coordination, and Operations. This construct suggests that policy and regulation, as stated earlier, will not be sufficient to realise the outcomes envisaged. Government needs to reach down into the national ecosystem and optimise the intelligence sharing, control and coordination mechanisms, and actual operations, including consequence management. The new National Office for Cyber Security, supporting the Commissioner, and the expanded capabilities afforded the new Cyber and Infrastructure Security Group, both within the Department of Home Affairs, will need to prioritise this effort and publicise their strategies and plans.

More carrot, less stick!

The core policy areas offer a solid start but are not sufficient. Regulatory frameworks not only need to be enhanced and harmonised but also simplified, with a much stronger emphasis on 'carrots', not 'sticks'. While strengthening Australia's international strategy on cyber security is important, so too is strengthening Australia's domestic strategy, which extends beyond securing government systems. Australian governments need to elevate the existing level of engagement with businesses and individuals through concrete steps to promote cyber

resilience. Government needs to promote improved technology standards, particularly in relation to cyber security.

Review and iterate the Strategy

The pace of change in the cyber threat landscape and the technologies means that the Cyber Security Strategy needs to be adaptable, and its implementation framework must be dynamic. This Strategy and especially its implementation framework *need to be subjected to continuous review and update*. To this end, actions, assessments and evaluations need to evolve with the threats and with developments across the national security and national resilience landscape. This review/adaptation cycle needs to be truly agile. It cannot afford to operate at 'bureaucratic pace' and each cycle should aim for a 70-80 per cent solution that is rapidly executed.

Outcomes over actions

The Cyber Security Strategy needs to acknowledge that cyber challenges are as much organisational as they are technical. Resilient cyber security must address both security capabilities (the people, infrastructure, and technology that is security-focused), and security processes (the culture, structure, policies, and other organisational elements that address how capabilities are used to achieve a desired security outcome). The Strategy needs to guard against a focus on "activity" versus "outcome".

Australia needs a CI-ISAC

The interconnectedness of critical infrastructure and the significantly increased numbers of Systems of National Significance (SONS) highlights both the importance of critical infrastructure and the need for a body that provides a dedicated community to ensure better collaboration with Government, all working together in a more consolidated way. A cross-sector Information Sharing and Analysis Centre (ISAC) would provide such a capability. It would help the nation think about issues, innovate solutions, and better understand one another across the public and private sectors.

The Critical Infrastructure - Information Sharing and Analysis Centre Australia (CI-ISAC) is operational and tackling this challenge. CI-ISAC has its first tranche of members representing more than half the SOCI CI sectors and it will continue to grow. Government has the opportunity to accelerate the work of CI-ISAC through partnership and funding support.

Priority Outcomes

CI-ISAC believe the Strategy should prioritise the following outcomes:

- Improving public-private mechanisms for cyber threat sharing and blocking.
- Supporting the creation of central 'turn key' capabilities that can support all entities.

- Supporting Australia's cyber security workforce and skills pipeline.
- National frameworks to respond to major cyber incidents.
- Community awareness and victim support.
- Investing in the cyber security ecosystem.
- Designing and sustaining security in new technologies.
- Implementation governance and ongoing evaluation.

PART 2

Completing our homework: Some responses to the Discussion Paper's focus questions

Responses to the framing questions are provided where we are confident that we have the expertise and experience to make a meaningful contribution.

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

One of the core policy areas is for government to address the harmonisation of regulatory frameworks. Businesses have been urging the government to harmonise the regulatory environment for months to help improve understanding of cyber security expectations across both the public and private sectors, which is reflected in the discussion paper. More needs to be done to explain cyber security obligations at the operational level and at the Board level for businesses. Many organisations that come under the Security of Critical Infrastructure Act definitions have not even heard of the Act, which means compliance regimes will have little effect and heavy-handed impositions could drive them out of business.

The notion of a new Cyber Security Act that draws together cyber-specific legislative obligations and standards across industry and government calls out for an improved industry response in the critical infrastructure sector. Industry needs to take more of a lead in this and be better supported by Government in doing so.

The cost impact on different businesses based upon their maturity, size, complexity, market, ownership and other factors may vary significantly. It is important that any reforms introduced maintain competitive neutrality and specifically do not disadvantage Australian owned companies and particularly Australian Small to Medium Enterprises (SMEs).

Further developments to the Security of Critical Infrastructure Act are clearly necessary, in particular including customer data and systems in the definition of critical assets, rather than just operational elements, to ensure data breaches like those experienced by Optus and Medibank are covered.

It is also important to note the recent Australian Productivity Commission report's findings that industry stakeholders observed that the SOCI Act was rushed, which did not allow for suitable consultation and resulted in apprehension and confusion in government processes.

As the new Cyber and Infrastructure Security Group within Home Affairs works to ensure that Government and industry cooperate together on hardening Australia's critical infrastructure and economy from cyber attacks and from other hazards, and supports the National Cyber Security Coordinator in cyber incident response and coordination, a cross-sector Information Sharing and Analysis Centre such as the CI-ISAC would be a highly valuable asset. Furthermore, such a Centre would complement the National Office for Cyber Security as it responds to cyber incidents, and as it provides a rapid capability to manage the consequences as they start to emerge.

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

and

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

and

Question 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?

These three questions all relate to international relationships; however, they also apply to the Australian national sphere, and especially to other national legal systems where Australia has treaty-making influence.

Internationally, there are excellent examples of approaches to how Australia has contributed to international standards-setting processes in relation to cyber security, and shaped laws, norms and standards that uphold responsible state behaviour in cyberspace. In fact, Australia has a history of leadership in this regard at the UN, with other Five Eyes nations, in Estonia, the APEC region, and elsewhere. While much of this has fallen under DFAT, specifically the Ambassador for Cyber Affairs, the international relations work should continue, either through DFAT or through new entities and roles being created in government. The resulting work, however, needs to have the force of law as mandatory rules that regulate behaviour, and not remain merely a statement of norms.

In relation to state behaviour, the work undertaken in Estonia which resulted in the Tallinn Manuals 1 and 2, and which recognised that international law applies in cyberspace and to cyber operations, should be properly recognised as an authoritative source of law, rather than

just the view of independent experts. This may be brought about through bi- or multi-lateral treaties.

More generally, in achieving international consensus on acceptable behaviours and norms in cyberspace, it would be beneficial to follow a similar approach to that adopted in the late 1990s that resulted in the model laws and conventions that recognised and facilitated electronic communications and transactions and which gave legal recognition to electronic commerce and communications. This would achieve large-scale consensus as to what constitutes acceptable behaviour in cyberspace. Whether or not this involves re-visiting the Cybercrime Convention of 2001 and/or the Russian-led 2019 resolution on cybercrime[1] that could result in irreversible consequences for how countries deal with and cooperate in cybercrime investigations or not remains to be seen, but should not be neglected.

Broadly speaking, acceptable behaviour is defined largely by law – both civil and criminal. The raft of Australian laws should be formally recognising as applying to cyberspace. If a body of research similar to Tallinn 1 and 2 was undertaken into the application of Australian national law to cyberspace and based on the over-arching interpretive nature of the electronic laws of the 1990s, there would be an enormous reduction in the need for new laws. (See more on interpretation below).

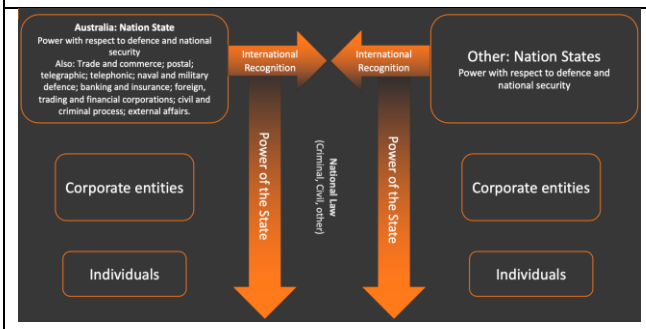
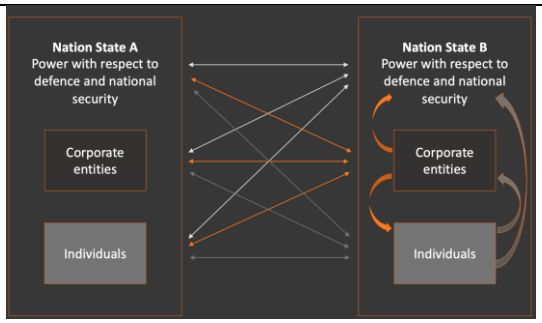
Breakdown in the Structure of Legal Order

Historically, public international law has governed the relationships between sovereign states and international organisations largely on the basis of equal recognition in a horizontal power structure. National laws have governed the relationships between one sovereign state and the juristic and natural persons in that state. Here the power structure is vertical, state power over persons.

The internet has changed this simple vertical and horizontal structure of legal order because the persons of one state can be proxies for that state (as seen with Fancy Bear and Russia) and can adopt the power of a sovereign state against another (a Russian private sector person vs sovereign US). Similarly, where North Korea acts against Sony Corp. (sovereign North Korea vs a private sector US person), neither the law that governs international relationships between sovereign states, nor the national law within a state applies.

The diagrams below help to explain this change.

[1] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/383/43/PDF/N1938343.pdf?OpenElement

Pre-internet order	Internet dynamics
	

In essence, these adversary actions have created 'diagonal' and uncertain legal consequences. One such consequence is that new laws such as the SOCI Act amendments authorise the Australian state to 'operate' private sector businesses in the defence of Australian persons (owners and operators of critical infrastructure) and the Australian state. This begs the broader question of whether adopting such National Security powers to run critical infrastructure business operations, including material supply chains, was ever meant to be a function of the state.

International treaties are powerful in helping to understand the structures of legal authority, especially when adopted into national legal systems as the basis for what constitutes acceptable norms of behaviour; just like unauthorised access (a re-interpretation of trespass in property law) was adopted into the criminal law of some 67 states through the Cyber Crime Convention of 2001.

An international solution is needed to solve international problems. It is not helpful for 67 States to have 67 cyber security laws, and the convergence of international and national legal systems needs to be better accommodated.

<u>Australian Federal Regulatory Regime</u>

The Cyber Security Strategy and substantive legal reforms underway in data privacy and protection (AGD) and telecommunications (DoHA) law should be well aligned. Clear responsibilities should be established in an effort to simplify the functions, powers and overlaps of ministerial portfolios (AGD, ACCC/Treasury) and regulators (ASIC, APRA, OAIC, etc).

The section 51 Legislative powers of the Parliament in the Australian Constitution should be considered in the light of comments above on interpretation, and that s51(v) "*postal, telegraphic, telephonic, and other like services*" include the internet. Similarly, s51(vi) that the "*naval and military defence of the Commonwealth and of the several States, and the control of the forces to execute and maintain the laws of the Commonwealth*", and s 51(xxxix) "*matters*

incidental" might be interpreted to include cyberspace, simplify national security, and increase legal certainty.

More on Interpretation

In *Microsoft Corporation (Plaintiff) vs John Doe 1-2 Controlling a Computer Network and thereby Injuring the Plaintiff* and its Customers (Defendants),[2] aside from unauthorised access[3] the Plaintiff successfully relied upon the unlawful use of Microsoft's Intellectual Property, as trademark infringement and passing off in relation to 'spearfishing'. Other causes of action included common law of trespass to chattels, unjust enrichment, and more. The Court orders included that the domain registries utilised for the criminal offences registered in the US be transferred to Microsoft, and requested that overseas registries, do likewise. This use of existing law demonstrates the scale and reach of what we have and should be using. This approach, including actions of estoppel in response to legal claims would work equally well in Australia and other countries, demonstrating the efficiency of relying on existing law and overarching interpretation.

This approach would simplify Australia's complex regulatory regime and ease the passage to implement the Cyber Security Strategy 2023.

Future Questions and Strategic Adaptability

There was a time when humans, women, children and animals had no rights. At this present time, 'things' have no rights. It is conceivable that they will, and even that they will enter into legal relationships with persons or with other things. We are also likely to soon see the 'melding of human, thing and artificial intelligence. The Cyber Security Strategy 2023 needs to begin with this end in sight. It is only by adopting the legal norms of hundreds of years of human experience described in international and national legal systems – the things that we know work - as the basis for future possibility that we can grow, on a solid foundation, into the future, relying upon purposive interpretation.

In summary – laws regulate human behaviours and relationships. Laws establish norms. Laws establish standards (even at common law), and all of these should apply in cyberspace *mutatis mutandis* as they do in other domains – land, sea, air, and space.

[2] Alexandria Division. Case 1:22-cv-00607-AJT-WEF *SEALED* Document 16 Filed 05/27/22. https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf

[3] Computer Fraud and Abuse Act, 18 U.S. Code § 1030.

<u>Question 7</u>. What can government do to improve information sharing with industry on cyber threats?

Government needs to use its unique position and resources to share aggregated threat information, work with industry at all levels of maturity to build their capability, and empower them to take the necessary protective and resilience actions. The ACSC's Cyber Threat Intelligence Sharing (CTIS) initiative supports machine-to-machine sharing of threat intelligence but most businesses do not have such a capability and more contextual threat information is needed to uplift their cyber defences.

A national cyber threat alerting system for a cyber-related attack or incident should be developed. Government should be in a position to take direct action to protect industry in the national interest, including in assisting businesses to take technical action to defend and protect their networks and systems. Furthermore, Government would be in a strong position to provide advice on mitigating damage, responding to the incidents and carrying out remediation activities,

Clarity around the governance framework for Government assistance is needed, including proportionality thresholds, and the reasonableness and practicality of actions. Furthermore, all levels of government and all industry sectors need to provide structured support, communication, and coordination to assist recovery efforts in the event of a cyber-incident.

A key issue in discussing critical infrastructure protection (CIP), when a lot of it isn't necessarily under the government's direct control, is how to protect the middle range of CIP players? In any vertical there will be "big" players who can afford to protect themselves, but there is frequently a middle tier of players who are critical and who can't afford to do all that they should to protect themselves.

The US notion of an Information Sharing and Analysis Centre (ISAC) allows the most logical entity to provide managed services to members of each CIP vertical who potentially couldn't otherwise afford higher levels of sophistication. Vulnerabilities and risk profiles are comparable across sectors. While international ISACs have evolved to address this challenge by providing a broad suite of capabilities tailored to the unique requirements of each sector, they don't take a cross-sectoral approach and are not necessarily as holistic and as inclusive as they could possibly be. These protections could be further supported by investing in building central 'turn key' capabilities (technical and procedural) within the ISAC that entities could use to rapidly speed up their own cyber maturity and defensive capabilities.

Critical infrastructure protection is a material area of national security risk, and owners and operators need support as they manage national security risk – support from Government and support from within Industry. An ISAC would help the larger organisations provide leadership and support to the smaller ones through sharing cyber threat intelligence and building a collective cyber defence posture. The varying levels of maturity across the 11 sectors needs to

be addressed – finance and telecoms sectors are very mature, which has been imposed on them through legislation and regulation. All sectors need to be uplifted.

Thus, an ISAC represents an opportunity for the critical infrastructure industry to self-organise and for its members to manage their own challenges — engaging with Government – in improving Australia's cyber defences. The strength and utility of any ISAC is directly related to the number of members it brings together and the diversity of insights and knowledge that these members bring to the ISAC's intelligence-sharing platform.

Contextual threat intelligence sharing and collaboration and communication across all critical infrastructure sectors is key to building a collective defence posture. Other capabilities can be added from this initial base, such as reporting and compliance support and cyber-security support.

What is needed is a highly-trusted omni-directional sharing, bringing together the cross-sectoral approach to augment Government initiatives such as CTIS and the Trusted Information Sharing Network (TISN). The CI-ISAC can provide this.

The CI-ISAC would be the sector hub for critical infrastructure, facilitating resource pooling, expanding access to support, and improving overall cyber posture. Above all, it would improve the quality of analysis and information sharing. The network effects of a large, cross-sectoral ISAC would benefit members by leveraging mature players to build turn-key capabilities which can be used to assist less mature, financially constrained industry members and accelerate their cyber maturity. This, coupled with central supporting functions, would consolidate expertise, and maximise utilisation of highly skilled and low-density cyber professionals. It would offer economies of scale and efficient utilisation of central expertise.

Furthermore, the CI-ISAC can pick up the load of sharing unclassified cyber threat information in near-real time across Australia's critical infrastructure community. This would include mitigation measures and cyber-security best practices that can help bolster critical infrastructure participants' cyber-security posture, as well as threat analysis that helps critical infrastructure members develop mitigation strategies. This is relevant in terms of the US Defence Industrial Base cyber program where participants are encouraged to report information and share cyber threat indicators that they believe are valuable in alerting the Government and others in order to better counter threat actor activity. While the Australian DoD (ACSC) does not have the size to offer a full DoD Cyber Crime Centre (DC3) that is the program's operational focal point, an ISAC that reached across all critical infrastructure sectors would bolster ACSC's ability and capacity to share unclassified cyber threat information in near-real time and respond to adversary and criminal activity.

While industry would invest in an ISAC, some public funding and grant mechanisms would be useful to help seed an industry-led ISAC. Government could also assist in informing and

facilitating the maturation of an ISAC by helping to remove barriers to sharing and collaboration around capability uplift.

The sharing of threat information is based on STIX / TAXII, which are the industry standards for cyber threat intelligence. STIX (Structured Threat Information eXpression) is a standardised language which has been developed by MITRE in a collaborative way in order to represent structured information about cyber threats. It has been developed so it can be shared, stored, and otherwise used in a consistent manner that facilitates automation and human assisted analysis. TAXII (Trusted Automated eXchange of Indicator Information) is a collection of services and message exchanges to enable the sharing of information about cyber threats across product, service and organisational boundaries. It is a transport vehicle for STIX structured threat information and key enabler to widespread exchange.

Government and industry are in a co-dependent relationship with respect to cyber security, which depends on a deep understanding of technological innovation and robust information sharing by both. Understanding the complexities of this and having a mature dialogue about roles and interdependencies will take time. Improved dialogue and involvement of all relevant parties will lead to better articulation of government and industry roles in cyberspace with sufficient granularity to operationalise their efforts.

Question 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?

An obligation of confidentiality may improve organisational support for sharing information during a cyber incident; however, this would by the nature of the agreement inhibit the ASD from then sharing the information it has received to benefit or support other organisations that may face the same cyber threat and thus not improve whole-of-nation cyber defences.

It is for this reason that a trusted, non-governmental mechanism that has no direct link or obligation to regulators acts as an intermediary to support the validation, enrichment and contextualisation of information from organisations experiencing cyber incidents.

We would see this as an additional enabling ecosystem working alongside any enhanced confidentiality agreements between the ASD and regulated private sector entities. The practicalities of enacting MOUs/Deeds/Agreements with all private sector entities would be material and time consuming as internal legal teams review indemnifications, etc.

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

and

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

Both these questions indicate the need for an improved focus on education. Education is vital, and action should be taken to ensure the Australian Curriculum addresses cyber security more profoundly through all tiers of education, including its importance in assuring continuity of business. Achieving an enhanced baseline understanding and awareness of cyber security is crucial for Australia's workforce.

Establishing and building on such a baseline would improve the ability for Government to deliver a comprehensive, multi-year program of workshops, exercises, information-sharing sessions and assessments to complement and inform sector and sub-sector-based assessments in Industry.

More effective pathways for interaction between government, government bodies, research institutions, industry sectors, and entrepreneurs are needed to build a better analytical capability as Australia benefits from research and emerging technologies. Through such pathways, Australia can develop the expertise, tools and systems to improve preparedness for, response to, resilience, and recovery from cyber attacks. More flexible employment options are needed for people to move between Industry and the public sector on multiple occasions.

Building the cyber workforce to make Australia the most cyber secure nation in the world by 2030 requires training the next generation of cyber-specialists and providing them a robust training environment that is agile, scalable and tailored to their unique learning needs. A ready cyber workforce must be supported by highly trained individuals who can access a variety of training tools on demand with intuitive interfaces. Moreover, this training environment must be able to accommodate team dynamics — either for a full team or a diverse range of smaller teams — for high fidelity training and mission rehearsal. And this training and exercising environment needs to straddle the various sectors to deal with multi-sector challenges.

Australia's businesses will need to improve the ability of their cyber workforce to: identify skills gaps; identify critical roles needed for the next one to three years and out to 2030; and address learning and skills needed in the next one to three years and out to 2030. Furthermore, building an effective cyber workforce is a journey that relies upon continuous growth and improvement. Any cyber-security training program for the nation should have flexibility to adapt to rapidly changing situations, new missions and adaptive threats. This will lead to a ready and proactive cyber workforce.

Finally, as with the technical capabilities mentioned to support collective defences, a suite of supporting programs and resources could be developed to support businesses in developing these newly trained cyber graduates through relevant career pathways within their organisations.

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

In relation to supporting major cyber incidents, the key to helping impacted organisations is making specialist resources available to reduce the time to contain the incident, ascertain the impacts and commence recovery activities to resume services/mitigate data exposure. In many (data-related) exposure situations, the 'horse has bolted' once the incident is reported; however, containment, impact assessment and recovery can still be supported.

All of these activities can be supported by (1) government specialists and (2) industry if facilitated via a trusted intermediary. The network effects of crowd sourcing information and support resources if coordinated well should not be discounted as a cyber incident response strategy. This approach is proven across other hazards and natural disasters and there is no reason it cannot be applied to cyber, provided the coordinator is an entity trusted by industry.

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

The rules that protect and support Australians should keep pace to the extent possible with the extreme rate of technological change and the changing nature of the threat environment in both traditional and rapidly evolving sectors of the economy. This demands a more dynamic approach to setting and adjusting laws and regulations. Government should ensure any change delivers the largest long-term benefits for society while minimising any upfront costs for industry and individuals. Australia needs a more adaptable and dynamic way of updating rules and protections. The challenge for Government is engaging the public to reduce a particular threat vector (such as Huawei) when the market has not offered useful alternatives. While there needs to be cost-effective alternate technology solutions, more effort is needed in improving education and perhaps setting standards on reducing risk from the other parts of the commercial IT supply chain.

Industry in the broad and small and medium businesses in particular need assistance in maintaining compliance and identifying areas for improvement, with a preference for continuing engagement rather than enforcement – more carrots, less sticks. This would entail providing guidance and advice, validating compliance activities, sharing best practice information, and clarifying expectations and standards. In the critical infrastructure sector, there is a need for industry to support industry in this regard, particularly for entities to provide an enhanced situational awareness across interdependent supply chains, and other expertise more generally, and to build a collective cyber defence.

<u>Question 16</u>. 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.

and

<u>Question 17</u>. How should we approach future proofing for cyber security technologies out to 2030?

Both these questions indicate the need for policies to acknowledge the understanding of supply and demand from economics to ensure that demand for security drives the supply of more secure products and services. A trusted market is necessary - an open, transparent, diverse and competitive technology market, where vendors include cyber security protections as standard and buyers clearly understand any risks. Ideally, digital products and services should have security built in 'by-design', so that users do not need to have any expert knowledge, but they should still have basic cyber security awareness.

To support this, Australia must have visible and trusted industry standards. A lot more needs to be done in setting best practice cyber security standards, and while it is important to participate in international fora, it is vital to establish a suite of standards within Australia. More explicit specification of obligations is needed, including adhering to best practice cyber security standards that are endorsed and where necessary, developed by Government. An excellent example of this is the CPS234 standard applicable to Financial Services Organisations, a lightweight version that goes beyond the ACSC's Essential 8 and maintains a strong focus on collaboration and sharing threat-information to benefit all entities, which would be an excellent addition.

A stronger industry certification regime is needed, one that provides confidence that suppliers and providers of services have undergone an independent assessment process that confirms the technology and service levels they can provide. This should include performance and security, and be an ongoing process. To the extent that Australian companies are competing in a global market, it's possible that mandated mechanisms for building in security can make these companies non-competitive. This will need to be addressed.

Many Cyber Security services and technologies are cost-prohibitive to Australian organisations, originating from overseas and far exceeding local budgets. Building accessible services and technologies (similar to open source, or CTIS building a hardened Malware Information Sharing Platform (MISP) for instance) is a proactive way that Australian SMEs can work together to make capabilities more accessible. CI-ISAC plans to develop 'turn-key' capabilities to the benefit of its members; however, specific re-usable security controls/technologies could be built at a national level that support compliance with standards and benefit organisations by making these accessible without the significant financial hurdles. Government could take the lead on

supporting the development of these capabilities either directly or through a trusted partner such as CI-ISAC.

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

The Strategy needs to provide information that is forward-looking as Australia's evolving cyber security protection and resilience measures will need to adapt as threats and vulnerabilities change. While past experience and accepted practice are important, the legislation, regulation, codes and standards need to be highly responsive to changing circumstances and readily adaptable.

For a start, the new Strategy should set the groundwork for better preparedness, especially exercises and learning the lessons, while building a knowledge base to translate those lessons into hard solutions. It should foster a more curious mind-set as to how we think about issues, innovate solutions, better understand one another, and become more involved in collaboration. The Strategy should provide the catalyst for exercising what a catastrophic event might look like, how the nation would function, what roles the various parties would play, and how we would recover.

<u>Question 20</u>. How should government measure its impact in uplifting national cyber resilience?

Government needs to provide information to help guide Australian businesses in achieving cyber protection and resilient outcomes and that information must be optimised to support and inform strategic and operational decisions. This includes embedding security, protection and resilience in the forefront of business planning. Information needs to be provided in context.

Risk Management is an enduring and ongoing function. It is not just a plan but entails creating an environment for continually looking at and managing risk, which must be part of business as usual. Risk Management Plans (RMPs) are key to operationalise the SOCI Act and improve the maturity of all sectors. An ISAC reaching across the entire critical infrastructure community would have a role to play here in helping Government achieve this.

Any metrics or measures need to be outcomes focussed; measuring outcomes and actual uplifts and avoided incidents will ensure our collective focus is on activities that drive towards these.

Contributors

CI-ISAC Board Members and Strategic Advisors: Stephen Beaumont, David Sandell, Scott Flower, Helaine Leggat, Gary Waters and Simon Connor.