ITI Promoting Innovation Worldwide

ITI Comments on the Australia Cyber Security Strategy Discussion Paper

ITI appreciates the opportunity to provide feedback on Australia's *2023-2030 Australian Cyber Security Strategy Discussion Paper* (hereafter referred to as "the paper") and we are grateful for the chance to engage in Australia's Cyber Security Strategy development efforts.

ITI represents 80 of the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Nearly a quarter of ITI's members are headquartered outside of the U.S.

We support Australia's efforts to develop a forward-looking Strategy, and we would like to offer the following recommendations for your consideration, per the discussion questions posed in Attachment A:

- *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?*

To become the "most cyber secure nation in the world", we recommend Australia leverage ITU's Global Cybersecurity Index[1] as a useful and trusted reference that measures the level of commitment of countries to cybersecurity at a global level. Each country's level of development is assessed along five pillars – (i) Legal Measures, (ii) Technical measures, (iii) Organisational Measures, and (v) Cooperation – and then aggregated into an overall score.

More specifically, the Strategy does not mention the importance of allowing for the free flow of data across borders. This is especially important for cybersecurity purposes, as availability of diverse sets of high-quality security data is critical to develop, deliver, and maintain cybersecurity solutions. As cyber-attacks become increasingly more sophisticated leveraging automation and AI, the free flow of security data is essential for real-time cyber defence and to counter adversaries who do not recognise borders. As such, we encourage

[1] "Global Cybersecurity Index." *International Telecommunication Union,* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Australia to include reference to promoting policies and international agreements that enable the free flow of security data across borders.

We also encourage Australia to prioritise ICT supply chain security in its Strategy. Supply chains present an expanded attack surface, and therefore, can be an attractive target for cyber adversaries to infiltrate, compromise, exploit, or otherwise gain widespread and undetected access to organisations' networks and systems. The ICT supply chain faces a variety of continuously evolving threats – 188 have been catalogued by the United States' Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force), a public-private partnership aimed at producing actionable solutions to supply chain-related challenges. As such, it is important to maintain a focus on supply chain security and resiliency in the Strategy. We urge Australia to reflect its policy vision for securing the ICT supply chain, including how it will work with partners to foster resilience.

- *2(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)?*

There are several ways Australia can be effective in improving cybersecurity norms, beginning with further guidance around cybersecurity best practices. For example, the Cybersecurity Performance Goals issued by the U.S. Cyber and Infrastructure Security Agency offers organisations a helpful baseline, allowing them to prioritise cybersecurity actions that will be most useful in addressing cyber risk and building a rudimentary cyber strategy.[2] A similar type of guidance document could be a helpful step in establishing common baseline cyber practices across sectors. We also note that the U.S.'s National Cybersecurity Strategy emphasises secure by design and secure by default practices and highlights the notion of rebalancing responsibility, which are also concepts that may be useful to explore.[3]

We recognise other countries are also considering regulatory approaches to foster a common cybersecurity baseline. While we appreciate these efforts are intended to improve cybersecurity across sectors, **it is important that such regulation is appropriately scoped and targeted to reflect varying risk profiles**. If Australia pursues a new *Cyber Security Act,* it should therefore consider what outcomes it is trying to achieve with such legislation and to tailor it accordingly – is it to apply a common baseline or minimum standards across critical infrastructure sectors (beyond the obligations that are included in the SOCI Act), or is it to foster a baseline across all products and services that are being placed on the market?

[2] "Cross-Sector Performance Goals."*Cybersecurity and Infrastructure Security Agency,* https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.
[3] "National Cybersecurity Strategy." *The White House,* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

In considering developing new legislation, Australia should evaluate its landscape of existing cybersecurity policy and regulation to identify gaps that need to be addressed or duplication/conflicts[4] that need to be removed, so as not to create an overly complex regulatory landscape.

Overall, improving cybersecurity requires a multi-faceted approach that includes education, training, and skills development; raising awareness at the executive and board-levels; cyber threat information sharing; promoting a prevention-first mindset; and, for governments, instituting effective legal regimes to deter and prosecute cybercriminals. In this way, Australia should emphasise all these potential levers in their Strategy. The Strategy should also emphasise that cybersecurity is a shared responsibility among all stakeholders. Suppliers/vendors should design and equip products and services with the strongest security in mind, update their products and services, and conduct due diligence in risk management to the extent possible. At the same time, end-users, including businesses and consumers, should recognise that their behaviour and specific use/application of a given product is instrumental in contributing to security.

- *2(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?*

There is an existing definition of "asset" in the SOCI Act[5]. In the data sector, there is also a business-critical data definition of personally identifiable information for instances of more than 20,000 individuals. As such, there is already some coverage of both customer data and "systems". Reforming the Act further to cover recent incidents exposing citizen identity data would not align with the original definition of "critical infrastructure" in the Australian Critical Infrastructure Resilience Strategy Plan 2015. The Australian Privacy Act reforms (discussed later) would be a more logical Act to ensure appropriate security of those asset types.

In addition, the current definition of 'critical assets' in the SOCI Act already places an undue burden on service providers. If the definition was expanded further, it would place an even more disproportionate burden on service providers. Including customer data and undefined 'systems' within the definition would only increase existing confusion as to responsibilities between asset owners and those owners' third-party service providers who may operate a specific function for the asset.

[4] The Australian Legal Information Institute and other leading Australian universities have called out evidence regarding this risk. See https://austlii.community/wiki/CyberLaw.

[5] In Section 5 of the SOCI Act, the definition of an "asset" includes a system, network, facility, computer, computer device, computer program, data, premises and "any other thing."

A key area of concern that remains in the final Act – and one that global industry voiced many times during the Act's negotiation - is the 'System Information Software' Powers. The Act states that system information software can be installed where the Secretary believes that a Systems of National Significance (SoNS) entity is not technically capable of otherwise provisioning system information itself. **However, this section of the Act does not clearly define or identify "SoNS". We had previously encouraged the Australian government to offer more explicit criteria that the Minister may consider in making such a determination to help alleviate uncertainty as to whether an asset may be considered a SoNS** and allow critical infrastructure owners and operators to be appropriately prepared for additional obligations. We continue to recommend the development of such criteria.

Additionally, we remain concerned with the fact that entities can be required to provide information to the Australian Signals Directorate (ASD) via this monitoring software for up to 12 months. This request can operate in conjunction with rolling and multiple 'system information periodic reporting' and 'system information event-based reporting'. This may lead to companies surrendering the data of their cybersecurity providers and cloud service providers without appropriate context, which may result in misinterpretation or incorrect use of the data. Although the system information is intended to exclude personal information captured under the Privacy Act, the system information laid out in the Explanatory Memorandum is sensitive in nature and the powers are substantial.

We also continue to recommend that the SOCI Act be amended to make clear that a vendor who provides a private cloud (i.e., the entity owns the asset, but the customer has full-control and is consuming it aaS), **is not by that virtue a direct interest holder and thus reporting entity**. Right now, the rules appear to only take into consideration traditional, public cloud vendors. For example, the "moneylender" exemption to the direct interest holder provisions, although somewhat addresses situations where the vendor provides a public cloud, appear to be too narrow.

The SOCI Act places obligations on "responsible entities" which – in particular for registration and reporting – may be duplicative or even conflicting in situations where there are arguably multiple reporting entities. A common example is where one entity owns and operates an asset but relies on service providers to perform various operational activities for the asset which may bring those providers into the definition of a responsible entity. The possibility of multiple reporting entities for the same Critical Infrastructure Asset (CIA) creates unnecessarily duplicative obligations and risks regulators receiving conflicting information. These risks are particularly attuned for cyber incident reporting and would be exacerbated should the number of 'critical assets' exponentially increase to include customer data and assets.

The Act should be clarified to establish only one responsible entity for a CIA. Where the responsible entity utilises third-party service provides to assist in operating the

asset, certain security obligations under the Act may rightfully flow down to such providers through the responsible entity, but the registration, reporting, and other obligations involving interaction with the agency should be limited to the entity which owns the asset.

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

No. This would likely overlap with the generic directors' duties in the Corporations Act which state that directors must remain informed on all risks that could impact the business.

- *2(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?*

We applaud the Australian government for creating a Coordinator for Cybersecurity as well as a National Office for Cyber Security within the Department of Home Affairs. We believe this is an important step in ensuring that the government takes a harmonised approach to cyber security. Indeed, any approach that is non-design neutral, globally fragmented, or otherwise duplicative of existing regimes may hinder companies' global competitiveness and innovation in technology and security solutions. In general, measures should be informed by fundamental security policy principles such as design neutrality, facilitating interoperability and scalable harmonised approaches to security (leveraging international standards and avoiding state and federal fragmentation), supporting private-public partnerships, favouring evidence-driven, risk-based approaches to security, and avoiding duplicative or localised requirements (e.g., in the domain of security certification) that may stifle growth and innovation to address ever-evolving cyber threats. Streamlining and harmonising cybersecurity policies will enable government to leverage the best available cyber defensive capabilities and provide government leadership with the information needed to make informed, risk-based decisions on security.

As an initial action, the National Office for Cyber Security ('Office') should survey the landscape of existing cybersecurity policy, including that which applies to the federal and state enterprise as well as to the private sector. This will equip the Office with an understanding of where there may be overlap or duplication of requirements and allow staff to more easily work to deconflict them. A good example of a body that is working to deconflict specific cybersecurity measures is the Cyber Incident Reporting Council, established under the U.S.' Cybersecurity Incident Reporting for Critical Infrastructure law passed in 2022.[6] The Council is chaired by the Under Secretary for Homeland Security and is comprised of several federal agencies with equities in the cybersecurity space, including

[6] "Readout of Inaugural Cyber Incident Reporting Council Meeting." *U.S. Department of Homeland Security,* https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting.

Office of the National Cyber Director, Federal Bureau of Investigation, Securities and Exchange Commission, Federal Trade Commission, Federal Communications Commission, and Departments of the Treasury, Defence, Justice, Agriculture, Commerce, Health and Human Services, Transportation, Energy, and Homeland Security. It is working to evaluate existing cyber incident reporting policy across U.S. federal agencies, with the goal of streamlining such policy to allow for a consistent and clear approach.

The Strategy should also align with parallel reforms to Australia's privacy framework. The Attorney-General Department's recently published Privacy Act Review Report introduces a detailed set of proposals that will require careful consideration from both a privacy and data security perspective. ITI welcomes the Report's proposals for further consultation with industry to streamline multiple data breach reporting obligations and better align the objectives of the Office of the Australian Information Commissioner (OAIC), Australian Cyber Security Centre (ACSC), and other concerned Government entities.

As such, the Strategy should lay out a clear process for evaluating, streamlining and deconflicting existing and proposed regulations, including how the Government will engage with the private sector.

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

The Government should follow the position of many other nations in seeking to bring ransomware attackers to justice and to recover from such attackers all extorted funds, but not prohibit ransom payments by victim entities except in situations where the payment would be made to a known sanctioned entity. Where a victim has cyber insurance coverage for the ransom payment, the use of such insurance should remain allowed. The reality persists that ransom payments are in many situations the sole means by which a victim entity may timely restore operations or obtain critical stolen data.

There is an important step that Australia can and should take related to ransomware not mentioned in the consultation document: Australia is already an active participant in the new global International Counter Ransomware Initiative (CRI), which brings together more than 30 governments plus the EU and Interpol to discuss and develop concrete, cooperative actions to counter the spread and impact of ransomware around the globe. **Australia has taken on a leadership role as inaugural chair and coordinator in spearheading a new International Counter Ransomware**

Task Force (ICRTF), which aims to develop a framework that will deter attacks and disrupt the ransomware business model.

The Australian Government should invigorate its work on the ICRTF, including building out the ICRTF platform that will enable like-minded countries and other stakeholders to securely share actionable information and best-practices to counter ransomware attacks.

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

Broad and consistent public education on cyber hygiene and best practices is one of the important first lines of defence in network security. Consumer awareness regarding the importance of multi-factor authentication, software updates include patches, and awareness of phishing and other tactics used by hackers to access networks is foundational and should not be underestimated. Along with bolstering public awareness around cybersecurity, ITI would also advocate for increased funding and promotion of Science, Technology, Engineering, and Math (STEM) education in Australia. Producing strong STEM students is not only valuable for creating the next generation of cybersecurity professionals, but increased funding can also help to promote vocational and mid-career education programs for STEM.

More broadly, the cyber skills discussion needs to move beyond cyber roles, and towards whole of Australia cyber literacy. Legislators, boards, business directors, and householder literacy are all just as important. In every organisation, security is everyone's responsibility. This requires organisations to help educate everyone. Cyber literacy in business leaders, government and regulators is a key gap area that requires focus.

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

Australia has an important opportunity to elevate itself as a leader in cyber security while deepening its collaborative relationships. Cybersecurity is a global imperative and is not something that one nation can tackle alone, so partnerships with likeminded countries are crucial. Countries around the world are actively creating or revising existing cybersecurity policies, particularly legislation pertaining to critical infrastructure owners and operators. For example, the European Union has come to an agreement on the Network and Information Security 2 (NIS2) Directive, while the United States released its National Cybersecurity Strategy and continues implementation work stemming from Executive Order 14028, *Improving the Nation's Cybersecurity*. An important component of many of these revisions is the addition of mandatory cyber incident reporting obligations, which in some cases, conflict with laws passed in other countries. Indeed, the incident reporting obligations imposed on critical assets as a part of the Security Legislation Amendment of 2021 differ from those passed as a part of the U.S. CIRCIA law and are

similarly not aligned with those imposed under NIS2. It will therefore be important for the Australian Cyber Security Strategy to not only explain how it will coordinate cyber policy across the Australian Government, but also explain how Australia can best engage with counterparts overseas to ensure that cyber policies are aligned to the best extent possible will be immensely helpful to avoiding a fragmented cyber ecosystem.

Leveraging existing multilateral and bilateral fora is one way that Australia can seek to build upon its existing cybersecurity leadership, but also coordinate with likeminded nations to ensure that cybersecurity requirements are aligned to the extent possible. For example, Australia plays a key role as one of the four partner countries that participate in the Quadrilateral Security Dialogue (Quad). Indeed, we note that the Quad has already agreed to discuss how to identify and evaluate potential risks in supply chains for digitally-enabled products, as well as work to align software security standards for government procurement. Bringing other ideas to the table in this forum may also be a helpful way to demonstrate leadership while also allowing Australia to share information on proposed cybersecurity reforms with its partners.

Australia should also continue to deepen its relationships with likeminded partners via formal mechanisms like bilateral cyber dialogues and share information about what it has learned throughout its process of cyber security reform. Partners can also exchange views and share best practices via these types of dialogues, learning from each other as to what sorts of policies and proposals have worked and why, as well as which ones may not have seen as much success. We also believe that Australia should further leverage its international partnerships to address issues relating to the location of data and service operations in an effort to align Australia's approach to cybersecurity with trusted international partners. Indeed, a more open landscape for operations of data and cloud-based services will allow for operational resilience and cost efficiencies. There should be a focus on lowering cost and easing the adoption of cyber security capabilities to significantly increase uptake across the economy.

Finally, to promote Australia as a cyber leader, the Government should seek to deepen its efforts around cybersecurity capacity building. Offering capacity building opportunities to developing countries, particularly those that neighbour Australia, is an important way to instil cyber security best practices and increase cyber resilience across the board. This also speaks to question **3** above, which asks about how Australia can work with neighbours to bolster cyber resilience and better respond to incidents.

In all these international activities, it is essential that Australia coordinate with and involve the private sector to the extent possible. This can ensure that goals are aligned, that efforts leverage industry's expertise, and that (based on that expertise) policies can effectively contribute to greater cyber security - and do not unintentionally stifle innovation.

- *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 cyberspace?*

In setting out its Cyber Security Strategy, Australia should continue to emphasise the important role of internationally-recognised cybersecurity standards in facilitating interoperability of approaches and securing cyberspace globally. Cybersecurity standards (like the ISO 27000 series) developed by Joint Technical Committee 1 (JTC1) of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have guided the global IT industry for 35 years. Informed government participation from agencies with interest and expertise in standards can help to support cybersecurity leadership in this and other standards bodies. Ministries within the Australian Government should consider how to involve technical experts more directly in the standards development process, recognising that standardisation should remain industry-driven.

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

A key action is to better operationalise threat sharing partnerships with trusted companies. The Government also should commit to allowing and promoting the free flow of security data (which includes cyber threat data) across the Australian border.

- *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?*

We recommend that the Government devote its efforts to disrupting the ransomware networks and threat actors, as opposed to focusing on the question of notification. Specifically, Australia should work to make the new International Counter Ransomware Task Force (ICRTF) an effective tool in this work.

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

Two essential best practice models are the automation of security operations centres (SOCs), and leveraging the reach of telecom carriers/ISPs to deploy enterprise-grade cyber security.

First, successfully protecting against automated attacks means we must incorporate automation into cyber defences, including security operations centres (SOCs). This levels the playing field, reduces the volume of threats, and allows for faster prevention of new and previously unknown threats. Automation also supports real-time incident response at scale to triage and respond to attacks faster. Artificial Intelligence (AI) and Machine

Learning (ML) can detect previously unknown threats based on their characteristics or behaviours at scale. This offers much more robust protection against threat activity. Automating SOC functions can also significantly benefit staffing -- low level threats are addressed by automation freeing up highly skilled (and finite) resources to address more sophisticated attacks. If an organisation or agency is unable to build their own SOC, they should be encouraged to leverage Managed Service Providers (MSPs). Some entities lack the cybersecurity maturity to run effective security programs internally. Increasingly, such entities should rely upon managed service providers to achieve a reasonable level of security.

Second, the vast majority of cyber-attacks leverage the networks of telecommunications carriers and Internet access service providers (IASPs). Given their enormous reach economy-wide, telecom carriers and IASPs can play an instrumental role in blocking threats at scale by using technologies to automatically detect and stop threats in real time that traverse their networks. Automation at this level can bring advanced scalable protection to an entire customer base, which is particularly important for customers such as small firms and everyday Australian citizens that lack the skills or resources to provide for their own security in the face of increasingly sophisticated cyber threats.

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

Yes. A single portal for reporting cyber security incidents would benefit both industry and regulators, particularly if the reporting elements are harmonised. Reporting entities face an ever-increasing number of reporting requirements, often with very prompt deadlines, vague and conflicting requirements for the initial report, and a wide-range of reporting mechanisms. Unifying all Australian reporting obligations into a signal portal would increase efficiency for entities during an often-stressful time, increase the accuracy of information provided, and reduce the risk of conflicting and duplicative reports for regulators to sort through. A focus on automation capabilities around all reporting will allow for greater efficiencies.

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

The United States' Cyber Safety Review Board[7], created as a part of EO 14028 referenced above, may be a useful model as Australia considers methods to evaluate and learn from cybersecurity incidents. The Board investigates major cyber security incidents/events and make recommendations to improve cybersecurity in both the public and private sector. The Board is composed of both government and private sector representatives, ensuring

[7] "Cyber Safety Review Board." *U.S. Cybersecurity and Infrastructure Security Agency,* https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb.

that a diverse set of perspectives and insight is considered. A similar set-up may be useful for Australia to consider in driving collaboration between the public and private sector while allowing for effective post-incident review.