15 April 2023
Department of Home Affairs
Brindabella Park
Canberra, ACT, 2600
Submitted online via webform at homeaffairs.gov.au

RE: Submission in Response to the Discussion Paper – 2023-2030 Cyber Security Strategy

Palo Alto Networks appreciates the opportunity to provide a submission in response to the Department of Home Affairs' call for views via the discussion paper on the 2023-2030 Cyber Security Strategy released in February 2023.

Palo Alto Networks is the global cyber security leader, securing the networks and information of enterprise and government customers to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cyber security posture. We work with some of the world's largest organisations across all industry verticals, including across governments and critical infrastructures.

We commend the Government for its leadership on cyber security, both nationally and internationally, particularly following several significant and challenging cyber incidents that occurred in Australia recently. We appreciate the Government's ongoing willingness to engage stakeholders in developing its Cyber Security Strategy and associated laws and regulations via a public consultation process.

Below we provide an overarching summary and our responses to select consultation questions. In answering the questions, we have drawn on Palo Alto Networks extensive cyber security policy and operational insights in Australia and other countries with similar objectives in securing and building trust in their digital infrastructures.

GENERAL COMMENTS

The new Cyber Security Strategy offers a unique opportunity to put in place a policy framework that builds upon established cyber security best practices and industry-developed state-of-the-art capabilities that strengthen Australia's cyber resiliency. Given that the cyber threat landscape will inevitably evolve during the strategy's timeframe, it is equally important to implement cyber security strategies and policies that can mitigate emerging, yet unknown, cyber threats.

We highlight and summarize the following recommendations that we elaborate on in our responses below, and that we believe should be included in the new Cyber Security Strategy:

- Promote Zero Trust (ZT) principles as well as attack surface management (ASM) capabilities to deliver cyber security that is proactive and cost-effective. As businesses and society as a whole become ever more dependent on information and communications technologies (ICT), and the capabilities of cyber adversaries continuously evolve, ZT and best-in-breed AI-enabled cyber security solutions offer the most comprehensive cyber security strategy for all organizations. ASM capabilities, in particular, can also be leveraged for near real-time impact monitoring of existing cyber security regulations and help assess the nation's cyber resiliency.

- Promote the adoption across businesses and Government agencies of industry-developed state-of-the-art AI/machine learning (ML) technologies to enable cyber defence at scale. AI / ML are currently driving real outcomes in cyber security and are foundational for the next generation of cyber security innovations. The indispensable value of the responsible use of AI / ML in cyber security has been recognized by other governments, like the European Union and the UK, promoting the use of commercially available AI / ML products and services.

- Promote policies that enable the free flow of security data across borders. The ability to transfer security data in real-time is critical to counter cyber attacks that are increasingly sophisticated and automated, launched by adversaries anywhere in the world and hitting targets in all countries. Effective cyber security requires connecting the dots between different threats and taking immediate action to deploy defences automatically. Having globally diverse security datasets is essential to train and deliver AI / ML-enabled cybersecurity solutions.

- Develop, together with industry, cyber threat risk frameworks that periodically assess the cyber threat landscape of emerging technologies and any gaps in cyber defence capabilities. The exponential pace of research, development and use of advanced technologies, such as AI and quantum computing, offer huge benefits for society and enhance our cyber defence arsenal. But it is equally important to proactively analyse how they are changing the threat landscape and enabling cyber adversaries to circumvent our best defences.

- Establish a new public-private governance that analyses major cyber events and informs the development of new cyber security policies. For example, a Cyber Safety Review Board (CSRB), similar to the board recently established in the US[1], is important to review major cyber events and make concrete recommendations that drive improvements across the public and private sectors. In addition, these reviews should be shared with CSRB-equivalent entities in neighbouring countries to strengthen overall regional cyber security.

- Leverage telecommunications service providers (SPs) and internet service providers (ISPs) to conduct threat blocking at scale based on enterprise-grade security. The vast majority of cyber attacks leverage the networks of SPs and ISPs. Given their enormous nationwide reach, SPs and ISPs 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.

- Prioritise ICT supply chain security that focuses on vendor practices and product integrity. As the operations of CI and many national security and defence platforms are increasingly digitised and connected, compromising underlying ICT supply chains can be an effective technique for cyber adversaries to gain widespread and undetected access to networks and systems.

- Streamline any overlapping and duplicative regulations to enhance the overall efficacy of the existing regulatory framework and bring down compliance and/or operating costs for Australian businesses. In addition, further, explore and use the Cybersecurity Framework (CSF) as the de facto risk management standard to help align the different regulations per industry.

[1] U.S. Cybersecurity and Infrastructure Security Agency, Cyber Safety Review Board (CSRB).

- Continue to spearhead the International Counter Ransomware Taskforce (ICRTF) as part of the International Counter Ransomware Initiative (CRI). The ICRTF brings together over 30 countries, and other stakeholders such as INTERPOL, to develop joint efforts to counter the spread and impact of ransomware around the globe.[2] In particular, we recommend global initiatives to disrupt the ransomware networks and threat actors and, as such, help decrease the number of organisations that are forced to make the difficult decision of whether or not to pay a ransom.

CONSULTATION QUESTIONS

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

We suggest the Australian Government promote Zero Trust principles and attack surface management - these are now cyber security baselines that have shown concrete efficacy and which all organisations should be adopting. Secondly, Australia should promote the free flow of security data domestically and internationally. Thirdly, Australia should undertake a nationwide campaign to raise awareness among all citizens of steps they can take to improve cyber security in their own lives. Fourthly, Australia should augment its "clean pipes" efforts to encourage service providers and ISPs to block cyber threats at scale. Lastly, we recommend Australia to promote the use of industry-developed state-of-the-art AI / ML products and services that enable cyber defence at scale, while also developing cyber threat risk frameworks of emerging technologies (6G, AI, and quantum computing).

Zero Trust (ZT) is a strategic approach to cyber security that secures an organisation by eliminating implicit trust and continuously validating every stage of digital interaction. Zero Trust is not a product but a security framework or principle that allows organisations to build resilience in their IT environments. We are yet to see any Australian guidance or advice on Zero Trust and would welcome the Australian Government's promulgation of this key security strategy.[3]

Attack surface management (ASM) is the process of continuously identifying, monitoring and managing all internet-connected assets, both internal and external, for potential attack vectors, exposures and risks. ASM is founded on the understanding that one cannot secure what one does not know. Attackers regularly scan the internet for vulnerabilities in public-facing infrastructure and exploit them. In today's world, it is critically important that organisations understand what their network looks like through the eyes of an adversary. Additionally, ASM capabilities are a useful tool to inform the Government on the impact of its existing framework of cyber security regulations (also see Question 22).

Promote the free flow of security data. The Australian Government should further explore mechanisms and approaches that promote sharing of security data to bolster cyber defences.[4] Security data is data

[2]https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative

[3] There is no mention of ZT in the ACSC's Information Security Manual (ISM), for example. The ISM, intended for CISOs, CIOs, security professionals and information technology managers, is a security framework organisations can apply, using their risk management framework, to protect their systems and data from cyber threats. The ISM briefly mentions network segmentation but does not expand on ZT principles, which go much further.

[4] Australia's Privacy Act Report currently also out for comment contemplates implementing authorities that would give the AG the ability to permit the sharing of certain information (with some protections/specifications) to mitigate the harm of a data breach - See Section 28.4 (P. 354).

relevant to, or used for, cyber security research, services or solutions such as the development of patches. It can include device and network information and other information such as URLs/Domains, session data, threat intelligence or data, and "telemetry data".

The ability to transfer security data in real-time is critical to counter cyber attacks that are increasingly sophisticated and automated, launched by adversaries anywhere in the world and hitting targets in all countries. The cyber security community leverages security data, combining cyber threat information from around the world to develop a global picture of cyber adversaries, including their techniques, tactics, infrastructure, and the like. Effective cyber security requires connecting the dots between different threats and taking immediate action to deploy defences against these threats automatically. Recent research from the Georgia Institute of Technology[5] and the Center for Information Policy Leadership (CIPL[6]) further highlights the potential harms of data localization policies with respect to cyber security, critical business operations and fraud prevention, amongst others.

As threats can originate from and target anywhere in the world, security data needs to be transferred freely in real-time across borders to understand best and counter the full range of cyber adversaries and the threats we all face. After all, our cyber adversaries do not recognise national borders. Data localisation policies that restrict the free and real-time flow of security data across borders can have serious and significant impacts on collective cyber security defence - including that of Australia. The Government should therefore look for mechanisms that help facilitate the flow of security data. Specifically, Australia should:

- 1) include in the new Cyber Security Strategy specific recognition and affirmation of the importance of the free flow of security data globally to Australia's cyber security;
- 2) account for network and information system use cases as officials update Australia's Privacy Act to ensure that Act does not inadvertently restrict the flow of security data;
- 3) take a leadership role with other governments to elevate the topic and gain commitments on free flow of security data globally.

<u>Collaborate with the private sector to launch a large-scale, national cyber security awareness campaign.</u> Australia has a history of large-scale, national campaigns to educate citizens of all ages about steps to take to reduce certain risks. Well-known campaigns include the "Click-Clack, Front and Back" campaign to reduce the death toll on roads, and the "Slip, Slop, Slap" campaign to promote UV protection and prevent skin cancer. These large-scale campaigns are undertaken at a societal level because there is a common risk to everyone. Cyber security, being a key priority in the national agenda, should be given the same attention. The Australian Government should work with the private sector to develop and launch a nationwide campaign to help Australians understand cyber security and cybercrime and the basic steps they should take to protect themselves. This campaign should address both the threat and provide simple measures that citizens can take to enhance their cyber security (this could be a simple message along the lines of "patch it up, back it up, lock it up").

<u>Promote the use of state-of-the-art AI / ML technologies that enable cyber defence at scale.</u> These technologies form the foundation for cyber security innovation. The indispensable value of AI / ML

[5] Peter Swire, DeBrae Kennedy-Mayo, The Effects of Data Localization on Cybersecurity, Georgia Tech Scheller College of Business Research Paper No. 4030905, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905

[6] The Center for Information Policy Leadership, The "Real Life Harms"of Data Localization Policies, March 2023, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

capabilities in cyber security is gaining recognition by other leading digital economies, like the European Union's recent adoption of the Network and Information Security Directive (NIS2[7]). Similarly, the recently released white paper from the UK's Department of Science, Innovation & Technology, "*A Pro-Innovation Approach to AI Technology,*" recognizes that AI's pattern recognition and recursive learning capabilities will be critical elements to address rapidly changing cyber threats. This and other societal-benefiting use cases are the reason why the UK government has identified AI as one of the nation's five critical technologies, which would warrant a pro-innovation approach to regulation.[8] In promoting the use of AI/Ml, the Australian Government should establish partnerships with and leverage global industry's massive investments in this space (rather than prioritise Government development of its own AI/ML security technologies, for example, that may not be as effective).

Develop cyber threat risk frameworks of emerging technologies (6G, AI and quantum computing). The rapid pace of research, development and deployment of advanced new technologies such as next-generation networks (e.g. 6G), AI, and quantum computing will impact Australia's society and economy for decades to come. It is imperative to consider not only how these technologies can benefit our cyber defence arsenal and innovation but also how they can change the cyber threat landscape and could circumvent our most cutting-edge cyber defences.

For governments, this involves working with industry and academia to assess the cyber security risks, balancing societal and security benefits of these innovations, and developing ways to mitigate the potential negative impacts of these technological advancements. We recommend developing periodic risk assessments of these emerging technologies in conjunction with the needed cyber security capabilities, as well as integrating concepts such as security-by-design and ZT in both the research and development (R&D) and deployment of these technologies.

Furthermore, Australia could lead internationally on this approach through influential forums such as the Australia-India-Japan-US Quadrilateral Security Dialogue ("Quad"), and also partner with for example, the European Union Agency for Cybersecurity (ENISA) that recently published a report on "Cybersecurity of AI and Standardization".[9]

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

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?

The 2022 reforms to the *Security of Critical Infrastructure Act* (Act) aimed at enhancing Australia's critical infrastructure resilience across 11 key sectors. At this stage, the Act is very early in its implementation phase, and it is difficult to determine the full extent of its effectiveness. As such, we believe this formative stage of the regulatory lifecycle would warrant the Government waiting to enact substantial reforms until enough time has passed to judge its effectiveness. At the same time, we have included

[7] Recital 51, Network and Information Systems Directive, Official Journal of the European Union.
[8] UK, Department of Science, Innovation and Technology, A Pro-Innovation Approach to AI Regulation.
[9] https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

below some specific recommendations for changes based on the Act's text and scope as written. We also respond to the second part of Question 2b about the definition of critical assets.

Recommended reforms to the Act:

Remove the 'System Information Software' Powers. The Act provides 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. 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'.

While we appreciate this is a 'provision of last resort', we do not think it appropriate, nor in the spirit of the Bill, that the Australian Government should be able to force private enterprises to install software on their networks. We recommend removing this provision for the following reasons:

- The installation of what constitutes third-party software has the potential to create vulnerabilities that could adversely impact the security of a SoNS entity and, by default, the Government's systems and client systems. Entities would need to review this software before putting it on their networks, which could take considerable time and effort. It is also unclear who would be responsible for ongoing product support and maintenance - including vulnerability management and patching. Finally, we note that this could expose the Government to liability for any adverse impacts arising from the installation of this software.
- The installation of software for monitoring purposes could expose sensitive data from cyber security services and products that in some cases may be unrelated to the scope and purview of the underlying information request and pass it through to the ASD. Without necessary contextualisation from the entity, this unfettered access could be misinterpreted and cause broader operational disruptions. Additionally, this level of access could expose information and systems from other entities in a provider's supply chain, which could complicate contractual duties and other standards of care between providers.
- The mandatory provision for installation of government software has the potential to adversely affect business interests and investment, as clients may doubt the system integrity of companies operating in Australia (as they may have this software on their systems). It also creates a precedent that may be copied by other jurisdictions and adversely impact Australia's interests.
- Our understanding of the Act's objectives is to achieve cyber security uplift and enhance national resilience. As such, we believe a better response to circumstances where an entity is not technically capable of providing system information itself would be to support the organisation to develop this capability in-house. This would create a true outcomes-focused partnership between the Government and SoNS entities.

Legislate an independent and expeditious appeal process for entities affected by Part 2C powers. It is reasonably foreseeable that the Government and industry may disagree with a course of action or decision taken in accordance with Part 2C powers. Given the broad nature of these powers, it is important that entities have an appeal mechanism available to them should they disagree with a government decision or request. We also note that these powers (and the current lack of review or appeal rights held by affected entities) may adversely affect Australia's attractiveness as a market for investment and the ability of Australian businesses to grow internationally. In accordance with Australian

values and principles, we encourage the Government to provide a legislated, independent and expeditious appeals process of all government powers granted under this Act.

Make key changes to the Act's security incident notification requirements. We would like to reiterate some previously raised concerns that have been echoed by many industry stakeholders when the Act was being developed. The expectation to report "potential breaches'' will result in overreporting of non-serious and non confirmed incidents. This in turn will strain resources for both industry and government and potentially decrease the level of utility by creating "white noise" that could distract from the more serious incidents. Where possible, incident reporting requirements should be harmonised with other jurisdictions' reporting requirements, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the United States.

Add Federal, State and Territory Government agencies to the Act's list of "Systems of National Significance". The Act designates two buckets of organisations: "critical infrastructure assets" and "systems of national significance" (SoNs) – the latter being a smaller subset of the former, and deemed most crucial to the nation by virtue of their interdependencies across sectors and potential for cascading consequences if disrupted. Governments (federal, state and territory) were not identified as either critical infrastructure assets or as SoNs under the Act. Given the importance of Government agencies - their data and functions - to our national and economic security, and social prosperity, we would encourage the Australian Government to designate all federal, state and territory entities as SoNs subject to the positive and enhanced cyber security obligations under the Act.

Our response to the question whether customer data and 'systems' should be included in the definition of 'critical assets':

No, it should not.

Adding customer data and systems would be a potentially large expansion of the law with an unknown security benefit. The term critical asset typically refers to those essential to an organisation's functioning and whose disruption or destruction can significantly impact operations, finances, and reputation. Data is contextual, as acknowledged in Australia's Privacy Act report currently out for consultation. Customer and systems data are undoubtedly valuable assets for any organisation, but including them in the definition of "critical assets" can have serious repercussions.

At the outset, a broad-brush regulation that includes customer and systems data in the definition of critical assets can lead to a culture of overprotection that stifles innovation by restricting the utility of an organisation's data. Organisations may become overly cautious and unwilling to experiment with new ideas and technologies for fear of damaging their critical assets. This can lead to stagnation and ultimately a loss of competitive advantage. As currently framed, the regulation protects those truly critical assets, which strikes a balance between risk and innovation.

Secondly, there are no known security benefits to including customer and systems data in the definition of critical assets. While it is important to protect customer and systems data from theft, loss, or unauthorised access, there is no evidence to suggest that additional restrictions would add protective benefits without degrading operational utility. Indeed, many organisations already have measures in place to protect these assets, such as encryption, access controls, and data backup procedures.

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

consequences?

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

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

As noted in our answer to Question 1b above, the reforms to the *Security of Critical Infrastructure Act* were only passed in 2022- and that Act has a plethora of new obligations. Australia should wait and judge its effectiveness before developing new cybersecurity legislation.

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?

Below we answer both of these questions.

How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security?

Regardless of the way the Government chooses to monitor regulatory burdens, it is important to keep in mind that organisations' professional cyber security assets are not fungible. There is already a shortage of cyber security professionals, and any time spent on compliance takes away from operations. Any measurement must consider the trade-offs that impact organisations' ability to secure their systems and data. For example, reporting compliance should not divert information security teams' sometimes very limited resources away from examining and remediating incidents and securing systems.

Are there opportunities to streamline existing regulatory frameworks?

Yes. We should revisit old/outdated regulations, and also address overlapping and duplicative regulations- not only are many of these less effective but they can raise operating costs for businesses, ultimately making Australia a less attractive/more expensive market for international investment.

Australia should leverage as a de facto standard the Cybersecurity Framework (CSF) developed and updated over the past decade by the US National Institute of Standards and Technology (NIST) in partnership with the global industry. The CSF is already leveraged by organisations worldwide (including the Japanese Government). Right now, in Australia cyber security regulations vary widely by industry. Adopting a CSF, or a CSF-based framework, could help establish a common baseline across sectors and raise standards across the nation.

While we highlight one duplicative/redundant area below for immediate action (certifications to sell into Government), the Australian Government may wish to establish more formal processes and structures to avoid duplication of policies into the future. The idea of creating a "Council of Technology Regulators" has been raised as a mechanism for leading and coordinating technology policy issues.[10] Regardless of process/structure to streamline regulatory frameworks, it is imperative that the Government consult

[10] https://www.innovationaus.com/labor-backs-call-for-a-council-of-tech-regulators-to-address-ad-hoc-policies/

with the private sector industry/affected entities. Such consultation should be a standalone effort– not solely in the context of this Strategy consultation or any one policy consultation (to do otherwise risks receiving feedback just from a select group of stakeholders responding to that single consultation).

A key example of redundant cyber security-related regulations relates to assessments/certifications to sell into the Federal Government. Under the previous Government, the Digital Transformation Agency (DTA) introduced the Hosting Certification Framework (HCF) as a requirement to sell cloud-delivered services into the Government up to the Protected level. The HCF now covers data centres and cloud service providers, and the Government proposes extending it to SaaS. However, Australia already has a complex mix of regulations, policies and accreditations that apply to SaaS solutions. In particular:

- The Defence-led Infosec Registered Assessors Program (IRAP) assessment is required to sell cloud-delivered services to the Government up to the Protected level. While IRAP and HCF look to address different risks, it is unclear how they would align - and in some cases they appear to have conflicting requirements (i.e with respect to the sovereignty of data).
- The recently amended *Critical Infrastructure Act* requires SaaS providers to provide detailed information about ownership structure and arrangements to the Department of Home Affairs.

While IRAP and the CI Act are overseen by the Defence and Home Affairs Departments, we believe they address the risks the DTA seeks to manage (assuming those Departments can share the relevant information with the DTA).

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?

We caution against a strict prohibition on ransom payment, at least in the near term. Instead, we recommend that the Government, together with other countries, work to disrupt ransomware networks; this can help decrease the number of organisations forced to decide whether to pay a ransom.

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

There are challenges inherent in barring payments. For example, there can be life-or-death situations such as a hospital that has its systems locked; in this case patient lives may be at risk if data and systems are not released/restored.

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?

To the extent that it is unclear, the Australian Government should clarify its position.

Additional comments on how Australia can contribute to disrupting ransomware: We would like to add additional commentary on how Australia can contribute to stemming ransomware.

Australia is already actively participating in the new global International Counter Ransomware Initiative (CRI). Launched in October 2021 in Washington DC, the CRI aims to bring together more than 30 governments plus the EU to discuss and develop concrete, cooperative actions to counter the spread and

impact of ransomware around the globe.[11] In November 2022 it was announced that Australia was taking a leadership role as inaugural chair and coordinator in spearheading a new International Counter Ransomware Task Force (ICRTF).[12] The ICRTF's goal is to create a framework that will deter attacks and disrupt the ransomware business model so that fewer organisations in the future will have to make the difficult decision of whether or not to pay ransom.[13]

The Australian Government should commit in the forthcoming Strategy to invigorate its work on the ICRTF, including building the ICRTF platform that will enable like-minded countries and other stakeholders to securely share actionable information and best practices to counter ransomware attacks. Palo Alto Networks is a partner in this work, and we welcome this opportunity to share our insights on cyber threat intelligence with the Australian Government to help inform the ICRTF.

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

Per our response to Question 14 below, Australia should establish a "Cyber Safety Review Board" to learn from organisations when a cyber event occurs. To the extent practicable, knowledge gained from such a Board could be shared with equivalent entities in other countries to raise collective cyber defences.

In addition, per our comment at the end of Question 2 above, Australia should continue to focus and build upon the global ransomware initiative it launched in November 2022. Australia also should continue cyber security discussions within the Quad (see Question 4 below).

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

Bilaterally: In the past, the Australian Government ran a series of Track 1.5 dialogues with various countries to strengthen official and unofficial diplomatic interactions between Australia and key nation states. Palo Alto Networks has participated in a number of Track 1.5 dialogues, including the Australia-US dialogue, and has found them extremely valuable. We suggest the Australian Government could work with interested industry stakeholders to determine if Australia's Track 1.5 series should be reinvigorated/ expanded with key nation states and industry stakeholders.

Multilaterally: We recommend Australia to continue and/or further promote cyber security as a top priority within the international policy discussions and agreements pertaining to globally shared interests in technology, security and economy. For example, the OECD, AUKUS, and Quad groups of nations of which Australia is a member. In particular, we recommend Australia (continue) advocating for international and public-private collaboration and agreements on ICT supply chain security, cyber security of emerging technologies, the free flow of security data and cyber security capacity building.

[11]https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative
[12]https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/
[13] https://minister.homeaffairs.gov.au/ClareONeil/Pages/australia-leads-global-task-force-to-fight-ransomware.aspx

Involve the private sector. In undertaking these bilateral/multilateral initiatives, the Australian Government should coordinate closely with the private sector, in recognition of the important role the private sector can play. The private sector can provide subject matter and technical expertise- this is particularly desirable in the context of specialised technical conversations, such as those pertaining to international technology standards, which often require expert knowledge. Not leveraging the industry's knowledge and input can lead to global efforts that– while well-intentioned- may not meet industry's needs or may unintentionally stifle innovation in cyber security. In addition, the private sector, where appropriate and aligned, can promote international topics, ideas and policies and be a valuable source on what topics, trends and issues might be of interest to certain countries and regions. Cyber security companies, in particular multinational ones, can help amplify the Australian Government's efforts internationally where appropriate, such as by supporting cyber security capacity-building initiatives.

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?

We are responding to the first part of this question regarding how Australia can better contribute to international standards-setting processes related to cyber security.

In short, Australia should promote industry-led, market-driven, globally harmonised ICT standards- including cyber security standards. Australia could play an important role in working with industry stakeholders, government counterparts in the region, and global allies to foster regular dialogues with the goal of ensuring consistent government approaches to supporting industry in the development of cyber security standards/best practices.

Governments- including the Australian Government- should avoid developing or promoting unique, country-specific ICT (including cyber security) standards that companies must use or build their products to. While often well-intentioned, this approach can harm innovation and security, largely because it runs counter to how the ICT industry works: the industry can create leading-edge, sophisticated, affordable products because companies can build one product version to voluntary, global, industry-led consensus-based standards that are accepted (or chosen) by the marketplace as the most effective or most appropriate. These products can then be sold globally, saving costs and raising manufacturing efficiencies. Diverting resources to meet country-specific requirements negates these benefits because companies must build tailored products and global product lines. This raises costs (ultimately to customers) and drains resources from research and development.

Focused specifically on cyber security, disparate, government-mandated technical standards may decrease security if they cannot keep up with constantly evolving threats. Mandated technical standards can also benefit adversaries who, knowing the defences employed, can circumvent them.

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

Here we have two general recommendations: 1) review the roles, responsibilities and cyber security investment across Government agencies and 2) prioritise ICT supply chain security that focuses on vendor practices and product integrity. We elaborate on each of these recommendations below.

Review the roles, responsibilities, and cyber security investment across Government agencies. Australia should ensure that all Government agencies have clear internal accountability and responsibilities for cyber security, are appropriately investing in cyber security, and are creating a security culture. We note that some Federal Government agencies do not have a Chief Information Security Officer (CISO) or similar role directly accountable to the Secretary or Agency Head. Instead, those responsible for cyber security may report to the Chief Information Officer (CIO) or the Chief Operating Officer (or in some cases both). It is critical that the CISO role has visibility at the highest level of the organisation to ensure that the cyber risks are appropriately understood and managed. This is particularly important given the objectives of a CIO and CISO may not necessarily align - as the CIO may want to focus on ease of access to information, where the CISO may be focused on the security of information.

The Government may also wish to review Secretary and Head of Agency responsibilities for cyber security. While directors of companies have some responsibility for managing cyber security risks, Secretaries and Heads of Agencies do not necessarily have similar obligations. Finally, the Government should undertake a review of security expenditure across Government agencies and consider breaking it out as a line item from more general ICT expenditures.

Prioritise ICT supply chain security that focuses on vendor practices and product integrity. ICT hardware and software underpin our national and economic security as well as our social prosperity, controlling the operations of power plants, telecommunications, medical devices and many national security and defence platforms. At the same time, as the world becomes increasingly digitised and connected, cyber attacks on ICT supply chains are on the rise. Compromising them can be an effective technique to gain widespread and undetected access to networks and systems. Unfortunately, cyber adversaries have been known to try to infiltrate the hardware and/or software development process to insert “back doors” or vulnerabilities for exploitation. These risks are particularly acute for the defence and national security communities, which depend on software for key data analytics and security functions.

The growing prevalence around the world of sophisticated supply chain attacks, like SolarStorm and Not Petya, has seen governments increasingly focused on identifying and mitigating risks within the ICT supply chain. In fact, efforts to disrupt or exploit supply chains have become, in the words of a senior US Homeland Security Department official, a “principal attack vector” for adversarial nations seeking to take advantage of vulnerabilities for espionage, sabotage or other malicious activities.[14] In this environment, strong supply chain security practices are key for governments globally to enhance their national security posture and resilience. We would therefore encourage the Australian Government to take stronger measures to manage and mitigate this risk via the following steps.

- *Establish dedicated Government resources focused on ICT supply chain security.* Australia should consider whether it has the appropriate policies, structures and processes to provide advice on high risk supply chain security issues and the appropriate levers to ensure that high-risk vendors are not embedded across Australian Government, at CI facilities, or within critical technologies.

[14] https://www.paloaltonetworks.com/blog/2020/06/policy-supply-chain-best-practices/

While many Government agencies have an interest in broader supply chain issues,[15] the Australian Government does not appear to have a centralised and dedicated ICT supply chain security or high risk vendor function to communicate across Governments (Federal, State and Territory), critical infrastructure assets and systems of national significance the risks posed by high risk technology products, services and solutions.[16]

- *Create a public list of high-risk products or vendors to enable risk-based decisions by public and private organisations.* This list could communicate to stakeholders across federal, state and territory agencies and critical infrastructure the risks of embedding certain technology products and services in their environment. As an example, the US Federal Communications Commission (FCC) maintains a list of high-risk companies "deemed to pose an unacceptable risk to national security or the security and safety of US persons."[17] All US Government agencies, and any CI project that receives public funding, are prohibited from using technologies/high-risk vendors on that list. This public list also advises and guides all US organisations and warns them against procuring certain technology goods and services from these companies.

- *Create a list of vendors that have disclosed their unique source code to foreign nations to enable risk-based decisions by all government agencies.* Increasingly, we have seen instances of countries implementing requirements—most notably, mandates to review or even hold source code—as a condition to sell technology to certain parts of their market. Widespread source code disclosure can actually weaken security since such disclosure can be leveraged to detect and exploit vulnerabilities in software used by organisations globally. Currently, the Australian Government does not have visibility as to whether technology and security companies it deals with have shared their unique source code with foreign governments—posing a potential security risk.[18] A list of companies that have shared the source code of their unique intellectual property with governments would support Government agencies in making risk-based decisions as part of its technology procurement decisions. A similar approach is taken by the US.[19]

- *Update the Commonwealth Procurement Rules and other key procurement policies to reference both cyber security and supply chain security.* We elaborate on this recommendation in our response to Question 18.

- *Establish practices and procedures to regularly review vendor practices and determine "red lines" for software removal.* While some organisations might examine how a vendor manages its software supply chain at the point of purchase, few would regularly review these practices. However, as we have seen from global cyber attacks, reviews of how vendors manage their software development practices may help organisations avoid exposure to supply chain attacks resulting from poor vendor practices. The government could collaborate with vendors of critical software on risk-based principles, including relevant changes to their software development practices. It should also consider a process for removing software from its environment.

[15] For example the Department of Industry, Science and Resources is looking at Supply Chain Resilience but this work is not focused on ICT supply chain security issues or security issues embedded within the ICT supply chain.
[16] This was also highlighted at the November 2022 Senate estimates hearing. More found here; https://parlinfo.aph.gov.au/parlInfo/download/committees/estimate/26359/toc_pdf/Legal%20and%20Constitutional%20Affairs%20Legislation%20Committee_2022_11_28_Official.pdf;fileType=application%2Fpdf#search=%22committees/estimate/26359/0000%22
[17] https://www.fcc.gov/supplychain/coveredlist
[18] https://www.aspistrategist.org.au/undetected-and-dormant-managing-australias-software-security-threat/
[19] https://www.govinfo.gov/content/pkg/BILLS-115hr5515enr/html/BILLS-115hr5515enr.htm

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

The Government can do many things to encourage greater threat information sharing- particularly the sharing of tradecraft and cyber-attack techniques. These include 1) operationalising partnerships with trusted companies, 2) building out a multi-tiered partnership model; and 3) expressly commit to allowing and promoting the free flow of security data across the Australian border.

Operationalise public-private partnerships with trusted companies to disrupt cyber adversaries and increase government visibility of the threat landscape. The Australian Government may wish to explore a proof of concept (PoC) for disruptive activities with a handful of trusted cyber and technology companies. Learning from this PoC could then be applied to develop stronger cooperation models at scale to disrupt cyber adversaries and increase Government visibility of the threat landscape.

Engagement with key cyber companies can offer the Australian Government both key insights and the ability to respond to cyber incidents rapidly. For example, Palo Alto Networks endpoint sensors observe 500 billion events per day. We analyse over 300 million files daily, maintain a malware repository of 16 billion samples, and maintain our own scan and NetFlow capabilities providing global visibility of the entire internet landscape (similar to that of the SIGINT system). Our unique visibility is equal to/complementary to that of the Australian Government. In terms of response, cyber companies are uniquely placed to support Government actions because we offer economies of scale by pushing out protections to our customer bases which can number tens of thousands of entities (if not more).

Recently, some governments have been seeking to enhance the operational utility of public-private partnerships and – in some cases – mature them to pursue joint coordinated defensive actions. This is commonly referred to as evolving from cyber threat 'information sharing' to 'information enabling.' The latter term means sharing information not for generic situational awareness but for the purpose of enabling a specific defensive or disruptive action.

Palo Alto Networks has a long track record of effective public-private information-sharing leadership that uniquely positions us to drive this evolution towards a more joint, proactive defence. We do not see information sharing as an end in and of itself. Rather, it allows us and our partners to bring our unique cyber defence capabilities and authorities to bear, resulting in arrest, sanctions, or costly infrastructure rebuilds for adversaries. Two prominent examples in the Australian context include:

- **Gallium:** In 2022, Palo Alto Networks Threat Intelligence Team, Unit 42, collaborated with the Australian Cyber Security Centre and the US National Security Agency to develop a report detailing the tactics and infrastructure used by a Chinese APT group, named "Gallium", who were targeting governments and critical infrastructure across Europe and Asia - including in Australia. The public release of this report, which detailed the infrastructure used by this group, forced the threat actor to abandon key capabilities and infrastructure.[20]

- **The Remote Access Tool (RAT) Trap:** Palo Alto Networks supported the Australian Federal Police's (AFP) Cybercrime Investigations Team, to identify and arrest a 24-year-old Australian man for allegedly creating and selling a Remote Access Tool (RAT), named Imminent Monitor (IM), to more

[20] https://unit42.paloaltonetworks.com/pingpull-gallium/

than 14,500 individuals across 128 countries. The AFP identified that 201 Australian individuals who bought the RAT were also named as respondents on domestic violence orders. One of these purchasers is also registered on the Child Sex Offender Register. This effort was part of a global operation which saw more than 85 warrants executed internationally, 434 devices seized (laptops, phones, servers, etc.) and 13 people arrested.[21]

Build out a multi-tiered engagement model for public-private partnerships. Consideration should be given to multi-tier engagement structures that group government and industry partners together in ways that best align to mission objectives and the nature of the desired relationship. We recommend that groupings be established around public and private sectors, and around the desired communication flows (unidirectional vs bidirectional). To expand, while some organisations may be consumers of Australian Government cyber threat intelligence (i.e some CI sectors and small-medium businesses), others (i.e. sophisticated technology/cyber security organisations) may be able to meaningfully contribute to the Australian Government's threat intelligence and support disruption efforts. The information and messaging around particular threats and vulnerabilities pushed out to these organisations should also be tailored depending on their level of sophistication.

We assess that governments that focus on developing operational collaboration with a small number (typically 10 or less) of the largest global technology and cyber companies are often best positioned to respond to the rapidly shifting threat environment. This benefit is typically tied to the global visibility, global reach, and impact on these organisations' greater cyber security ecosystem. At the same time, the Australian Government should forge strong relationships with leading companies in non-tech sectors to help disrupt activities unique to those sectors.

Expressly commit to allowing and promoting the free flow of security data across the Australian border
Many of us want to create an ecosystem of greater threat sharing, but we must be able to share threat information globally in real time for this to be successful. Our response to Question 1 explains why the free flow of security data is essential to cyber security.

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 for ASD/ACSC during a cyber incident could improve engagement and build trust with affected organisations, especially when concerns about information sharing with regulators arise. However, the obligation should be balanced with the need for transparency and accountability, allowing for exceptions only when necessary.

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?

[21] https://www.afp.gov.au/news-media/media-releases/afp-charges-man-creating-global-spyware-tool

Per our response to Questions 2f and 2g, we recommend that the Government focus its efforts on disrupting the ransomware networks, threat actors and business models and redouble its efforts 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?

We recommend two: automation of security operations centres (SOCs), and leveraging the economy-wide reach of service providers/ISPs to deploy enterprise-grade cyber security.

SOC automation. Today, cyber-attacks as well as cyber security defences leverage machine learning and automation.[22] If organisations try manual defence against automated attacks, the fight becomes human-versus-machine, with highly unfavourable odds for the human-driven organisation.

Successfully protecting against automated attacks necessitates incorporating 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. Automating SOC functions can also significantly benefit staffing - low level threats are addressed by automation, freeing up highly skilled (and finite) staff resources to address more sophisticated attacks.

Leveraging service providers/ ISPs to conduct threat blocking at scale based on enterprise-grade security. The vast majority of cyber attacks leverage the networks of telecommunications service providers (SPs) and Internet service providers (ISPs) - Australia is no different. Given their enormous global reach, SPs and ISPs can play an instrumental role in blocking threats at scale by using technologies to 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 security in the face of increasingly sophisticated cyber threats.

Automated, at-scale cyber security will be critical as Australia moves toward 5G. As the Australian Mobile Telecommunications Association (AMTA) has stated, "5G is a key enabler for Australia, and will not only provide Australians with better connectivity, it will also impact all sectors of our economy and society and ultimately enable industries to become more productive and efficient, helping with the country's economic recovery following the global COVID-19 pandemic."[23] 5G is not simply faster than previous 4G or 3G networks. 5G's advantages–speed, latency improvements, greater agility, efficiency, and openness—mean it will be a major driver of digital transformation. Businesses increasingly leverage private 5G networks that allow for industrial-scale IoT networks with ultra-low latency, mission-critical reliability, and a high degree of mobility. Business and mission-critical applications for enterprise 5G will include use cases such as energy, utilities, critical infrastructure, manufacturing, mining, logistics, and fleet management. 5G also will be leveraged by government agencies, such as militaries, significantly enhancing mission readiness and enabling new capabilities across many environments — from campuses, logistics and military bases to aircraft carriers.

[22] An automated attack is one performed by a computer program (rather than the attacker manually performing the steps in the attack sequence).

[23] https://amta.org.au/acma-audit-reassures-5g-is-safe/

Because of the mission criticality of 5G, the approach to securing it must be much more sophisticated—what we call "enterprise-grade"[24]—than security that may have been sufficient for previous network generations. Further, the applications and services that ride on 5G networks are as critical to secure as the network infrastructure. Businesses and governments need security that can stop cyber attackers from infiltrating their networks, disrupting critical services, destroying industrial assets, or (in the healthcare field) jeopardising human lives.

Enterprise-grade security must leverage the following three capabilities.

- Zero Trust Security: We explain the Zero Trust security principle of "never trust, always verify" in Question 1. Extending Zero Trust security into SP/ISP networks can reduce the volume and impact of cyber attacks by ensuring that network elements act only according to their defined role and do not have unauthorised interaction or communication with other parts of the network or outside the network or by ensuring threats cannot move laterally in a network.
- Consistent, granular visibility of threats: Consistent, real-time granular visibility of threats passing through the networks is essential to stop those threats in real time.
- Automated security enforcement: Some examples are authenticating and automatically identifying devices and users before granting access to perform a certain action, such as requesting data. Automation is critical in responding to threats and taking action—for example, dynamically isolating infected subscribers and devices before botnet attacks can occur. The cyber security industry is making breakthroughs in ML and AI to detect and block the most sophisticated malware, network intrusions, phishing attempts, and many more threats.

There is precedent for this type of "at scale" model. At least one EU government has deployed firewalls across its entire national-level ISP infrastructure to protect its government, citizens, and businesses at scale from cyber attacks launched by various sophisticated state-based actors. In Australia, Telstra has an important "Cleaner Pipes" initiative based on Domain Name System (DNS) filtering, where millions of malware communications are being blocked as they try to cross Telstra's networks. DNS filtering should be complemented by additional steps and technologies to automatically block threats at scale before they execute into cyber attacks.[25] As such, the Australian Government should promote as a best practice prioritised enterprise-grade cyber security considerations and investments in SP/ISP network planning and build-outs as Australia moves to 5G. The Government also should collaborate with industry partners to promote the adoption of this approach- such as how SPs and ISPs can be incentivised to adopt such offerings. For example, such a capability could be made available to all end-users on an opt-in or opt-out basis. These measures can reduce the volume and impact of cyber attacks to national infrastructure, government networks, businesses, and citizens.

[24] More details are in *The imperative of enterprise-grade security for 5G*. Cybersecurity: A Peer-Reviewed Journal. May 30, 2022. See https://www.paloaltonetworks.com/resources/articles/cybersecurity-journal-imperative-of-enterprise-grade-security.html

[25] DNS filtering means that you are only seeing the traffic after a system in a business or household has been compromised. Some other limitations of relying solely on DNS filtering are that attackers can easily leverage or reroute to use another DNS service (malicious actors can create code to do this automatically as part of their attacks). Further, users can easily choose a different DNS provider that may not undertake filtering.

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

In general, yes, many cyber security skills are distinct from general STEM skills, and thus upskilling in cyber security is an important Government focus. We recommend the Australian Government partner with the private sector in uplifting cyber security skills- the private sector is already taking strong initiative and has extensive experience in this area. For example, Palo Alto Networks is committed to growing the next generation of Australian cyber security professionals via our Cybersecurity Academy Program (which, as of June 2022, had more than 30 Australian partners),[26] our participation in the Australian Government's Skill Finder Initiative, and our Cyber Safe Kids program in Australia.[27]

In addition, we should broaden the aperture of cyber security training to emphasise not just traditional incident response activities but also include programs that train our workforce in data science and other fields that will maximize our ability to utilize ML technologies in cyber defence. ML-driven capabilities have significant implications for the cyber workforce. Finally, the hundreds of thousands of open cyber security positions should be broken out into the job categories to identify the different skills and experiences needed to fill these positions (such as Tier 1, Tier 2, and Tier 3 analysts). Using automation for Tier 1 services that require little to no human supervision enables faster decision making and threat detection to support complex incident response and threat hunting activities. This evolution of security operations alleviates staffing pressures on SOCs that are spread too thin without compromising threat detection and response capabilities.

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

The Government can do the following related to education.

Fund Skill Finder. Skill Finder did not receive funding in the 2022 budget, and we encourage the Government to consider continuing to fund this initiative. Mico-credentials are increasingly important in addressing Australia's cyber skills challenge. Skill Finder brings together over 2000 free online courses provided by the world's leading technology companies.[28] Skill Finder helps to address our cyber security skills challenge by encouraging Australians to retrain/upskill into the security and technology fields, leveraging micro-credentials. Palo Alto Networks has a landing page on the Skill Finder website and links to our free Cybersecurity Academy courses (under the "cyber security" tab).

Consider Government scholarships for ICT and cyber security fields. The Australian Government may wish to consider Government-funded scholarships (both entry and post-grad level) to attract and incentivise people into the technology and ICT industry. Any financial incentive/scholarship could include a return to service obligation, ensuring graduates undertake a number of years in key government agencies (Home Affairs, ACSC and so on) at the completion of their paid studies.

[26] https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/education/apac-academy-list-june-2022.pdf
[27] https://www.paloaltonetworks.com.au/company/press/2021/palo-alto-networks-launches-cyber-safe-kids-initiative-helping-keep-aussie-kids-safe-online
[28] https://www.skillfinder.com.au/

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?

Whether or not a portal is the best mechanism, Australia should resolve duplicative cyber incident reporting obligations via a single reporting agency (we recommend the ACSC) and mechanism for all companies irrespective of the circumstances by which they have been breached or the nature of exposed/stolen information. This will relieve the regulatory burden placed on industry and help ensure the public and private sector work efficiently to protect our ICT infrastructure.

At least two Australian incident reporting obligations are duplicative and overlapping:

1) The Notifiable Data Breaches Scheme under the *Privacy Act* requires companies to report to the Office of the Australian Information Commissioner (OAIC) on breaches of personal information irrespective of whether it is the result of a cyber incident or human error (i.e. a data spill). However, should the compromise of personal information have resulted from a cyber incident, the company would also likely need to report to the Australian Cyber Security Centre (ACSC).
2) The recently amended *Security of Critical Infrastructure Act* requires regulated entities to report cyber incidents to the ACSC, even if the incident is not related to personal information. However, should the cyber incident impact personal information, entities must also report to the OAIC.

These two requirements leverage two different forms of reporting that must go to two different agencies and have two different reporting timeframes. As the Government reviews the Privacy Act, and considers adding IP addresses and other technical information to Australia's definition of 'personal information', the overlap and burdensome nature of this situation will likely worsen. Any steps to mandate the reporting of ransomware payments threatens to make the situation even worse.

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

Establish a Cyber Incident Review Board or Similar Forum. In May 2021, US President Biden established via Executive Order (EO) the Cyber Safety Review Board (CSRB). This board, composed of public and private sector representatives, serves an important function to review major cyber events and make concrete recommendations that would drive improvements across the public and private sector. In the wake of two significant cyber incidents, Australia may wish to consider establishing a similar forum. This board should be composed of trusted cyber security and other partners. It could be tasked with making public and confidential recommendations - depending on the incident - and should be scoped to review incidents affecting both government and industry.

A key feature of such a board is to provide an authoritative, trusted account of what happened, why, and what we should do about it. In the absence of such a body, fully dissecting significant cyber events often requires imperfectly triangulating a range of scattered insight. Accordingly, the CSRB in the US has often been compared to the US National Transportation Safety Board, a government agency which provides a

similar authoritative retrospective of aviation incidents.[29]

Besides this ex-post approach, and looking at the entirety of an incident lifecycle, additional value can be found in developing a (public-private) governance structure that enables effective communication and coordination among stakeholders during major events, as well as an (ex-ante) policy advisory committee that can preview and analyse future cyber threats and risks (as mentioned under Question 1). Taken together, this type of incident lifecycle governance can help support the Australian Government in the successful implementation of its national cyber security strategy.

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

Australia should leverage and continue to promote its new International Counter Ransomware Task Force/effort we highlighted in our response to Question 2.

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

See our answer to Question 10 about how SP/ISPs can leverage their economies of scale to block cyber threats that could impact small businesses.

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?

Government agencies should generally be held to the same account regarding cyber security as private organisations. In addition, the Government should mandate its agencies adhere to Zero Trust and attack surface management (we describe these concepts in our answer to Question 1, above). These concepts have been identified by the US government as imperatives, and US government agencies have been directed to implement them in their own environments. The Australian Government also should automate its security operations centres (SOCs). The Government should promote these three cyber security practices to organisations throughout the economy, as well.

Guidance and mandates requiring agencies to adopt zero trust (ZT). The Government should make the adoption of ZT mandatory for all government agencies. The Zero Trust model has become increasingly important for the US federal government due to President Biden's unprecedented Executive Order on Improving the Nation's Cybersecurity and the more recent federal Zero Trust strategy from the U.S. Office of Management and Budget (OMB).[30] Signed in the aftermath of multiple consequential cyber incidents, the Executive Order and OMB strategy lay out a series of actions that US federal departments and agencies must take to strengthen their cyber defences by the end of the US fiscal year 2024.

[29] https://www.ntsb.gov/Pages/home.aspx

[30] https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/.

Guidance and mandates requiring agencies to leverage attack surface management capabilities. We encourage the Australian Government mandate that each agency (at the Federal, State and Territory level) implement technologies to improve the real-time discovery of and visibility over its network attack surface - particularly its forward-facing internet assets and assets held in cloud environments. This would reduce the risk of exposures exploitable by malicious adversaries. This effort would align with government laws and actions promoting ASM emerging in the US and EU.[31]

Guidance and mandates on the automation of government SOCs to detect, prevent and respond to cyber attacks. Where appropriate, agencies should be required to automate their SOC functions to ensure the agencies can respond to threats in real-time. See Question 10 where we elaborate on SOC automation.

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

One approach is to leverage cloud-delivered security solutions. To defend at scale, at a national level, requires agility. As network architectures become more complex, security teams increasingly need help to adapt quickly and provide consistent security to all devices and data traversing networks and clouds. Cloud-delivered security services are a growing piece of most organisations' security strategies, enabling rapid scalability of protection with up-to-the-minute updates and simplifying the deployment and management of security. Cloud-delivered security services can be integrated with and amplify the efficacy of existing systems and workflows.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

The Government should better use its procurement as a lever to support and encourage the cyber security ecosystem for three key reasons. First, government networks simply need to be secure. Like all organisations, government ministries/departments must take appropriate steps to secure their networks and data. The Government holds a huge amount of the private sector's data; this is something about which, in many cases, individuals have no choice. The Australian government also holds a huge amount of national security-related information. All of this data and information must be securely protected. Government use of the best cyber security solutions, consistently, is key and will help protect the security and economic interests of the country as a whole. Second, the government can set an example for the private sector. Third, government procurement/purchasing power can drive good behavior among vendors such as end-to-end ICT supply chain security and product integrity practices.

Below are specific recommendations on how the Australian Government can do this.

Emphasise procurement of commercial off-the-shelf (COTS) ICT solutions. Several Australian Government agencies are still developing "in-house" ICT capabilities even when there are COTS solutions available. COTS solutions have many advantages, particularly in the cyber security space, as vendors typically invest significant R&D resources, and also often leverage global cyber threat intelligence to enhance the COTS products' capabilities. In an increasingly hostile threat landscape, it is

[31] For example, the US National Defense Authorization Act (NDAA), US Federal Information Security Management Act (FISMA) reform efforts, and the EU Network and Information Security Directive (NIS2).

imperative that the Government's finite cyber security resources are deployed to priority tasks, which may not include developing custom government ICT products, and instead leverage best in breed COTS security technologies. COTS solutions can also help Governments manage the cyber security skills challenge - skilled and cleared staff can focus on mission critical/priority tasks rather than maintaining or building custom-built government ICT solutions.

A particularly noteworthy example of government agencies leveraging COTS solutions for large-scale cyber defence operations is the US Department of Defense Internet Operations Management Program, which leverages the Cortex Xpanse attack surface management capability[32]. In this use case, Xpanse enables the US military to automatically identify its known and unknown internet-facing assets, prioritize them for remediation, and deploy playbooks to address critical vulnerabilities.

Update the Commonwealth Procurement Rules and other key procurement policies to reference both cyber security and supply chain security. Achieving value for money is the core rule of the Commonwealth Procurement Rules as it is critical to ensuring that public resources are used in the most efficient, effective, ethical and economic manner. However, it is important to remember that price is not the only factor when procuring goods and services. Government officials, particularly with respect to technology purchases, should be required to consider other non-financial benefits associated with procuring a certain product; in particular, the security of the technology in question and the product's integrity with respect to its supply chain security. Amending the Commonwealth Procurement Rules and various other policies to explicitly mention the importance of cyber security and/or supply chain security can help Government agencies gain value for money.

The Australian Government may also wish to consider the relevance of the March 2021 US Executive Order and accompanying guidelines which require US government agencies to purchase only software that meets secure development standards to protect government data.[33] These documents are intended to help agencies get the necessary information from software producers in a form that can help guide risk-based decisions and span many types of software, along with firmware, operating systems, applications and application services, among other things. The Australian Government should consider adopting and integrating similar things into its procurement policies and practices.

Procurement processes should include asking software companies about their product integrity practices and adherence to NIST's Secure Software Development Framework (described in footnote 33). This could include key questions about their internal processes and oversight mechanisms to mitigate the risk of modification during the development lifecycle and whether they undertake third-party testing to ensure that security vulnerabilities are identified earlier in the process.

We conclude with the recognition that Question 18 asks how to "ensure that there is a viable path to market for Australian cyber security firms." Palo Alto Networks supports Australian cyber innovation,

[32]https://www.paloaltonetworks.com/company/press/2022/palo-alto-networks-cortex-xpanse-to-supercharge-cyber-defenses-for-department-of-defense?utm_medium=social&utm_source=LinkedIn&utm_campaign=Cyber-Defense-Press-Release

[33]https://www.paloaltonetworks.com/blog/2022/04/software-development-standards/?utm_medium=social&utm_source=LinkedIn&utm_campaign=software-development-standards-blog. To support the order, the National Institute of Standards and Technology issued guidance that provides US federal agencies with best practices for enhancing the security of the software supply chain. Two guidelines were released: the *Secure software development framework* and the companion *Software supply chain security guidance*. The EO also directs the US Office of Management and Budget to take appropriate steps to require that agencies comply with the guidelines within 30 days. This means that federal agencies must begin adopting the framework and related guidance immediately while customising it to their agency-specific risk profile and mission. Vendors that supply software to the US government will soon also have to attest to meeting these guidelines.

and we collaborate with leading Australian cyber companies that are bringing the country's considerable capabilities to the market. We also believe we need more, not less, companies innovating and inventing new ways of combating cyber threats. However, we caution against enacting any protectionist policies that discriminate against non-Australian-owned companies. There are important ways governments can establish confidence in technologies regardless of where they are produced, such as by focusing on vendors' ability to demonstrate strong supply chain and product integrity practices. Relying exclusively on home-grown technologies will not be as effective as identifying vendors and technologies built upon the highest standards of product integrity and supply chain best practices. Further, h ealthy market competition drives innovation (and in fact we attribute much of our company's two-decade growth and success to the fact that we have had- and continue to have- fierce competition from around the world).

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

Regarding how to address the "cyber security of emerging technologies", see our response under Question 1. Regarding how to promote security by design: Australia has taken steps to reform the IRAP process, moving it from a "point in time" certification of ICT products to one focused on how vendors security design, develop, and manufacture their products. Australia should continue to prioritise IRAP reform in this direction.

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

We would advocate leveraging attack surface management capabilities to create a 'cyber weather' map that gives broad visibility into Australia's cyber security posture across specific critical public and private sector internet-facing cyber terrain. This type of near real-time monitoring can be a powerful tool to help evaluate the impact of cyber security laws and regulations and inform the direction of any reforms that may be needed to increase the nation's cyber resiliency and/or allocate resources to address critical vulnerabilities that remain visible to adversaries on networks.

CONCLUSION AND ABOUT PALO ALTO NETWORKS

We would be happy to discuss our ideas further. For more information, please contact Sean Duca, Vice President, Regional Chief Security Officer – Asia Pacific & Japan, at [redacted] or Martijn Nuijten, Senior Director, Global Policy, at [redacted]

About Palo Alto Networks

Palo Alto Networks is the world's cyber security leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cyber security to thousands of customers globally, across all sectors. Our best-in-class cyber security platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cyber security partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cyber security workplace of choice, recognized among *Newsweek*'s Most Loved Workplaces (2021), *Comparably* Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

Palo Alto Networks: Contribution to Australia's Cyber Security Ecosystem

Palo Alto Networks is committed to helping Australian Governments at the Federal, State and Territory level embrace the digital world safely and protect their operations from cyber attacks. We undertake a range of activities that contribute to strengthening Australia's cyber security posture, including actively supporting Governments at the operational and strategic level. We continue to share our cyber security expertise with Governments via policy submissions, and parliamentary testimony and by hosting strategic roundtables to promote thought leadership and discussion on key government policies.

In addition to our policy work with Governments, Palo Alto Networks is also committed to growing the next generation of Australian cybersecurity professionals. We provide Australian academic institutions with curriculum, technology, and faculty training at no cost via our Cybersecurity Academy Program, and as of June 2022 more than 30 Australian institutions were Academy Partners. We are also a member of the Australian Government's Skill Finder Initiative - which provides free access to over 2000 online courses provided by the world's leading tech companies.

Finally, Palo Alto Networks undertakes activities across our community to raise cyber security awareness and engage the next generation on cyber security issues. With a mission to become the cyber security partner of choice, we launched our Cyber Safe Kids program in February 2020. This program aims to educate students aged 5-15 on the skills they need to protect their digital future and become good digital citizens. Palo Alto Networks stands ready to support Australian Governments to make each day safer and more secure than the one before. For more information see https://www.paloaltonetworks.com.au/ or Palo Alto Networks Contribution to Australia's Cyber Capability.