27 August 2021

Cyber and Critical Technology Division
Department of Home Affairs
Submitted Online

RE: Submission in Response to Call for Views on *Strengthening Australia's Cyber Security Regulations and Incentives*

Palo Alto Networks appreciates the opportunity to provide a submission in response to the Government's call for views on the *Strengthening Australia's Cyber Security Regulations and Incentives* (this or the Paper).

Palo Alto Networks is the global cyber security leader, securing the networks and information of more than 85,000 enterprise and government customers in 150+ countries 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.

We congratulate the Australian Government for its leadership on cyber security matters to date. We appreciate the Government's willingness to engage stakeholders in the development of cyber security policy. Below we offer some general comments regarding five recommendations not explored in the consultation, followed by answers to some select questions in the Paper.

GENERAL COMMENTS

Recommendation: Assess the Impacts of Pending Regulations Before Exploring Further Regulations

We note the Australian Government is pursuing a number of significant and concurrent regulatory agendas relevant to this Paper. Two of these are the *Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the CI Bill)* and the review of the efficacy of *the Privacy Act 1988 (Privacy Act)*.

The CI Bill contains a suite of measures intended to uplift the cyber security resilience of Australia's critical infrastructure across 11 different sectors. The Bill contains several measures relevant to this Paper. These include, but are not limited to, board-level reporting on cyber security and supply chain risks, an expanded definition of critical infrastructure, and mandatory cyber incident notification requirements. These measures will not only elevate cyber security to the board level, but they will also have flow-on impacts across the economy - as companies regulated by the Bill would seek assurances from other companies in their supply chain as to their cyber security posture and resilience. It is also worth noting that the Bill does not prescribe that a company be of a particular size in determining whether it is a regulated critical infrastructure entity. As such, the Bill will not just capture large companies but also small and medium enterprises (SMEs) who may deliver critical services. Some have estimated that the CI Bill will impact 80% of the Australian economy. Given the anticipated impact of the CI Bill, we would recommend assessing its impacts and any follow-on standards or requirements, before introducing any new regulations aimed at uplifting cyber security across the economy.

The Australian Government's work to review the efficacy of the Privacy Act, and efforts to bring the legislation in line with international best practice will have impacts relevant to cyber security. For example, the Government is reviewing the current exemptions under the Privacy Act, and other organisations may be brought into the Act's purview. This would likely result in cyber security uplift amongst a broader cohort, as they align their practices with the Australian Privacy Principles, including data breach notification requirements.

Given that both of these aforementioned reforms are likely to have far-reaching effects in terms of cyber security uplift across the economy, we would recommend the Government first assess the impacts of these reforms and undertake a gap analysis before proposing any further regulations in this space. This will avoid unintended consequences, avoid duplication and reduce regulatory burden on the affected companies.

Recommendation: Clarify the Problem and Reconsider Scope of the Paper

Related to the above, a number of the chapters in the Paper discuss regulation of "large" business (the term is not defined). However, larger businesses are already or will be regulated by a plethora of regulations - including the CI Bill. We would recommend that the Paper refocus on supporting SMEs with their cyber security uplift, particularly because the passage of the CI Bill may attract heightened attention from the larger business they contract with.

Recommendation: Incentives Over Regulations to Achieve Uplift

As the Government considers the feedback to this call for views, we would encourage it to focus on measures that incentivise industry, as opposed to regulate it. Creating and implementing new regulations can be slow, complex and costly. In contrast, incentives are generally welcomed by Industry and can be adopted into business practices and processes quickly. Incentives may offer the quickest way to uplift cyber security across the economy and do it at scale.

Recommendation: Incentives for Telcos and Internet Service Providers (ISPs) to adopt a Clean Pipes Policy to Uplift Cyber Security of the Economy at Scale

Palo Alto Networks believes that in order to reduce the economic impacts of cyber security incidents, Australia should harden its national defences and address these threats at scale via leveraging the ability of telcos and Internet Service Providers (ISPs) to detect and stop cyberattacks in real time. This approach recognises that the vast majority of cyberattacks that occur in Australia leverage Australian ISP or telco infrastructure. In particular, Palo Alto Networks supports the adoption of a national clean pipes policy and encourages the Government to work with Industry and play an active role in driving its adoption.

'Clean pipes' is the idea that ISPs could provide security services to their customers to deliver a level of default security. A key advantage of clean pipes is that it brings advanced scalable protection to an ISP's entire customer base, which is particularly important to the majority of customers who lack the skills and resources to provide for their own security - such as SMEs as well as everyday Australians. To ensure the necessary level of security capabilities clean pipes would be delivered by ISPs in collaboration with industry partners.

The Australian Government and the Australian Strategic Policy Institute (ASPI) have talked about clean pipes' merits, and Telstra has announced a clean pipes strategy. On 30 June 2020, Prime Minister Scott Morrison announced a funding commitment to 'prevent malicious cyber activity from ever reaching millions of Australians across the country by blocking known malicious websites and computer viruses at speed'.[1] The *2020 Cyber Security Strategy* went further to note the importance of businesses, particularly telecommunications providers, automatically blocking known malicious threats to protect Australians and Australian businesses from cyberattacks at speed and scale. It noted that the Government will, over the life of the Strategy, support businesses to implement threat-blocking technology that can automatically protect citizens and businesses from known malware and trojans. This would help prevent and minimise harm to organisations and Australian citizens who cannot protect themselves.

The Strategy also notes Telstra's "Cleaner Pipes" initiative announced in May 2020. Telstra should be lauded for paving the way with this initiative, which involves Telstra's Domain Name System (DNS) filtering, where millions of malware communications are being blocked as they try to cross Telstra's networks.[2] While there are limitations of DNS filtering as a technical solution to delivering what some might consider a more comprehensive clean pipes solution, this announcement is a great step in the right direction.

We recommend that the Government determine how it might broaden and scale a clean pipes approach, as well as provide incentives (economic or otherwise) for ISPs and telcos to take similar actions to help build Australia's collective defences. Specifically, Palo Alto Networks recommends that the Government look at ways to encourage and incentify ISPs and telcos to maintain constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cyber security threats within that traffic. Having this capability be

[1] Scott Morrison, 'Nation's largest ever investment in cyber security', media release, 30 June 2020
[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-panel

available to all ISP and Telco customers would be a great next step.

The capability to detect and stop threats in real time exists in the market today. However, these capabilities are not widely known or adopted. As ASPI notes in its recent paper ‘Clean pipes: Should ISPs provide a more secure internet?’, while there is ‘no legal impediment to ISPs providing some level of protection to their customers (excepting techniques that would be privacy-invading), there is also no incentive to provide these services.’[3] The paper also goes further to note that there is no community expectation that ISPs will deliver this service nor is there any ‘ legal or regulatory obligation that has pushed ISPs to provide enhanced default security services.’[4] Many of the end users that would benefit from a clean pipes policy (i.e. SMEs) are likely unaware that these capabilities exist and would not know to request it from their ISPs. For these reasons we believe that there is a role for the Government in driving these policies - as the market is unlikely to implement measures that will result in costs to the business without any incentives to do so.

The Government should consider as part of this review how it can incentivise and support ISPs and Telcos to provide these services to the broader community. A clean pipes solution is a key mechanism to protect Australian Governments, businesses and families from cyberthreats, and make Australia a less attractive target to cyber adversaries.

Recommendation: Use Existing Government “Levers” to Uplift Cyber Security

Palo Alto Networks notes that the Government has a range of existing levers it could use to incentivise cyber uplift across the Australian economy.

Firstly, the Australian Government should consider using its procurement power to drive change and improve cyber security resilience across the economy. As ASPI notes, an emphasis on cyber security across Government procurement ‘has the potential to be transformative, given the government’s huge procurement spend (81,174 contracts with a combined value of $53.9 billion were published on AusTender in 2019–20).’ [5] Having cyber security play a more prominent role in government procurement practices may help to lift standards across the economy - ‘as companies will be incentivised to lift their standards too qualify to do business with the government, and it will often be easier for them to apply those standards across their whole enterprises rather than just for their government contracts.’[6] Amendment to

[3] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet

[4] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet

[5] https://www.aspi.org.au/report/exfiltrate-encrypt-extort?__cf_chl_managed_tk__=pmd_vmBEo74oXnOQeCU9lzNgeDGNiLfiuZg38yGrexMnDJA-1630021897-0-gqNtZGzNAxCjcnBszQfR

[6] https://www.aspi.org.au/report/exfiltrate-encrypt-extort?__cf_chl_managed_tk__=pmd_vmBEo74oXnOQeCU9lzNgeDGNiLfiuZg38yGrexMnDJA-1630021897-0-gqNtZGzNAxCjcnBszQfR

Government procurement policies should not only address the cyber security posture of the companies they are procuring services from but also, strengthen reference to the cyber security and supply chain standards of the technology and goods the Commonwealth may be procuring. In particular, the Government should update its procurement policies (i.e. the Commonwealth Procurement Rules and the ASDEFCON Suite) to reference the importance of cyber security and supply chain security risks.

Secondly, the Government could consider expanding programs such as the Skilling Australia's Defence Industry Grants Program beyond the defence portfolio, to other core agencies and functions of government (i.e Home Affairs, Services Australia). This program provides grants to SMEs that service, or intend to service, the defence industry with the capacity and skills required to operate in that supply chain (including with respect to cyber security). A similar program could be introduced for organisations that feed into the whole-of-government supply chain to uplift cyber security resilience via both training and physical upgrades.

Finally, the Government may want to consider taxation incentives to support businesses with their cyber security uplift. A recent report from ASPI discussed the merits of cyber uplift via the temporary full expensing scheme, previously known as instant asset write-offs.[7] As it currently stands, cyber security assets aren't clearly defined, and only bespoke in-house software is covered. The Government may wish to consider broadening the scheme to include off-the-shelf products and subscription services (such as software as a service and cloud services). Consuming cyber security protections as a service (e.g. via the cloud) will allow the Australian organisations to adapt more quickly to evolving threats. A tax incentive would encourage businesses to move to the subscription services which may otherwise be deterred on the basis of time, money and effort.

SELECT QUESTIONS

Chapter 3: The current regulatory framework

What are the strengths and limitations of Australia's current regulatory framework for cyber security?
How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

In answer to both of these questions, please see our above comments regarding incentives for telcos and ISPs to adopt a clean pipes policy.

[7] https://www.aspi.org.au/report/exfiltrate-encrypt-extort?__cf_chl_managed_tk__=pmd_vmBEo74oXnOQeCU9lzNgeDGNiLfiuZg38yGrexMnDJA-1630021897-0-gqNtZGzNAxCjcnBszQfR

Chapter 4: Governance Standards for Large Businesses

What is the best approach to strengthening corporate governance of cyber security risk? Why?

We note here that the focus of Chapter 4 is on ways to 'encourage stronger cyber security risk management within *large* businesses' [emphasis added]. We reiterate that the pending CI Bill, will likely regulate or affect almost all large businesses in Australia. We anticipate that many governance issues raised in this Paper may be addressed via the Bill's requirement that the board sign off on risk management plans addressing cyber security, which in turn will be shared with the Australian Government. In line with the above comments, we recommend the Government assess the impacts of the CI Bill before introducing new regulations related to corporate governance, voluntary or otherwise, and consequently recommend the adoption of "Option 0 - Status Quo" until that assessment is complete.

What cyber security support, if any, should be provided to directors of small and medium companies?

The frequency and severity of cyber incidents on Australian SMEs is increasing. In 2017, one in four Australian small businesses were victims of cyber-crime (up from one in five in 2016) and the financial losses associated with these incidents increased to an average of $10,299 in 2017 (up from $6,591 in 2016).[8] While SMEs are increasingly victims of cyber attacks, reports highlight the low levels of cyber maturity in the sector; a 2017 survey found 87% of Australian SMEs reported believing that their business was safe from cyber-attacks because they use antivirus software alone.[9] These cyber incidents impact not only SMEs themselves - in terms of their reputation, profits and operations - they also impact their customers, who may have lost personal, business or financial information stored on the SMEs' systems as a result of the incident.

Often SMEs do not have the expertise, time or resources to improve their cyber security resilience. This is why the Government must focus on providing SMEs simplified and practical support - in addition to a level of default security provided by the national adoption of a clean pipes policy (see above).

In order to provide simplified advice and support at scale, the Government should work with Managed Security Service Providers (MSSPs), Cloud Service Providers (CSPs), ISPs and cyber security companies to identify and/or create tailored offerings for SMEs that are cost effective and provide holistic security, alleviating some of the technical burden currently facing Australian

[8] Norton, SMB Cyber Security Survey Australia 2017
[9] Norton, SMB Cyber Security Survey Australia 2017

SMEs. The Government could look to subsidise the cost of purchasing these offerings via an SME cyber security grants program or via tax incentives (as noted above).

Governments should also work with the private sector to educate SMEs, including their boards, on cyber security more broadly. This training should provide an understanding of basic cyber security risks and mitigations, educating SMEs so they can take simple measures to protect their data and network. There are already many free knowledge bases and courses, many developed by the private sector, that these SMEs can access and leverage; these should be compiled on a government website and promoted to these SMEs via government channels.

> Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Our experience is that most business leaders need to understand better what skills they actually need to get to their desired cyber security *and* business outcomes.

Most companies want to employ highly experienced Chief Information Security Officers (CISO)/Chief Security Officers (CSO) although they do not necessarily need one (or want to pay for one). A CISO's role can range from tactical/reactive, to proactive, to very proactive. For example, at the most tactical level, a CISO might seek to use the basic threat and vulnerability information, to do cyber hygiene. At the next level, a CISO might analyse if new threats apply to their organisation and have a response plan (still largely reactive). An experienced CISO might focus on resilience, cost to the business, and mitigation, and put these data into financial models. Finally, a highly experienced CISO will interact with the board and help to integrate cyber security into business decisions, such as mergers and acquisitions (M&As); this type of CISO usually has business knowledge. Deciding which type of CISO is required should align with an organisation's maturity and needs. However, a common and increasingly important need is that CSOs and CISOs across companies of all sizes possess business acumen and translation skills - supporting their boards and leadership teams to understand technical risks as business risks and vice versa. Business leaders and board of directors should treat their organisation's online assets with the same level of care and attention that they pay to their organisation's real-world assets. The CISO/CSO must ensure that the executive leadership team and the board of directors are aware of the risks posed to these assets and how the risks are being managed.

Some businesses may decide, appropriately, that they do not want a CSO/CISO. SMEs frequently will go this path and outsource/purchase security as a service. But managing outsourced security effectively still requires in-house expertise to best select those services. Someone in the business, regardless of title, will need to make decisions about what security services they want to purchase, and will be involved in negotiating the contracts and service-level agreements (SLAs). The business, no matter its size, should know its desired security outcomes and what is most important (for example, patch management, understanding the threat impact, attaining cyber resilience, etc). That desired outcome can then be integrated into the contract or SLA with the security provider, ensuring that the security services received meet the purchaser's needs and are in their best interests. Boards and leadership teams also need to understand that they are outsourcing responsibility, not accountability for their cyber security posture.

Identifying skills needed to reach a desired security outcome will enable a business to hire the right candidate (or promote/train the right internal person), give them the appropriate metrics of success, and maintain ongoing education and training appropriate to that role.

Chapter 5: Minimum Standards for Personal Information

Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

We question whether the Privacy Act is the most effective way to promote the uptake of cyber security standards across the economy. A code under the Privacy Act would not apply to some enterprises, as the Privacy Act has exemptions for companies who have a turnover of less than 3 million annually. This would mean that more than 30% of the Australian economy would not be covered by the Code. Larger companies are already handling personal information in a manner consistent with the Privacy Act and in many cases are also compliant with other robust international frameworks, such as General Data Protection Regulation (GDPR). Some of these companies will also be subject to, and impacted by, the CI Bill and the impacts of these regulations should be assessed before further regulatory action is taken.

What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

The security of personal information is important to Palo Alto Networks. We use appropriate technical and organisational security measures to protect information from misuse, unauthorised or unlawful access or disclosure, loss, alteration, damage or destruction. We understand the importance of technical controls to protect personal information.

Commonly deployed technology safeguards for securing personal information include the use of anti-malware, encryption, monitoring of systems and data centers, firewalls, encrypted channels, and secure communications software. However, we question the effectiveness of having prescribed technical controls as part of a cyber security code under the Privacy Act. A single methodology of security controls is not applicable to all situations or organisations and in fact could have the opposite desired effect of protecting personal information. Companies, regardless of the sensitivity and scale of personal information they process, may assume a false sense of compliance simply by adhering to a prescribed set of technical controls. The security controls applied to personal information should be commensurate and proportionate to what is being protected. That said, if Australia decides to include any technical controls in the Privacy Act, the Australian Government should ensure that any required controls align with the technical controls mandated under the European Union's GDPR, particularly the new technical measures required under the Standard Contractual Clauses (SCCs) issued by the European Commission on 4 June 2021 governing the transfer of personal data from the European Economic Area (EEA) to third countries pursuant to the GDPR. From an international standpoint, it becomes difficult and often confusing for both individuals and companies to adhere to multiple standards, regulations, and law. As the GDPR has become the de facto international privacy standard and many global organisations have designed their privacy and security compliance programs with the GDPR as the framework, Australia should ensure that any required technical controls aligns with the GDPR.

What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

If Australia pursues a code, we believe that de-identified, anonymized and pseudonymized information are sufficient and do not need additional protections and should not be covered under a code. These data present a limited risk, and it is important to acknowledge that the aforementioned privacy techniques and tools are already used by many organisations to protect and maintain personal information in a secure manner. Mandating additional protection on de-identified, anonymized and pseudonymized data will only serve to discourage the use of those tools and encourage more data to be saved in a personal form, which creates more privacy risks.

Chapter 6: Standards for Smart Devices

What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Palo Alto Networks recommends the Australian Government consider how it can develop and promote policies to secure IoT at the network level, in addition to the device level.

We stress the network level as a priority security enforcement point because IoT device security, while important, is often a very operationally inefficient approach that is prone to error, given the many issues encountered when trying to secure at this level (e.g. highly heterogeneous IoT device environments, poor or nonexistent product security/patch support from some vendors, and inability of some products to be secured directly). There is also the issue of legacy devices -

billions of already-deployed IoT devices that cannot be retroactively designed and certified.

Policymakers must look more holistically and promote security in both the network and the large ecosystem of companies that work together to deploy and run IoT systems. The network is a logical detection and enforcement point for IoT security, because all IoT devices leverage mobile/ISP networks to communicate. Australia should encourage organisations, private and public, to leverage technology to have complete visibility of their networks and to enable themselves to discover, identify, secure, and optimise their connected devices. To date, Australian policymakers have focused on the response, recovery and incident reporting of network providers. While this is important, we would also recommend that the Government promote detection and prevention of threats and incidents on networks. With investment in the right technology, and a focus on automation, a majority of attacks can be detected and successfully prevented in a cost-efficient and timely manner. Furthermore, applying Zero Trust network security principles helps ensure the widest protection surface. The Australian Government should launch a concerted effort to determine how to approach IoT security at the network level. Efforts to secure IoT at the network level should be promoted in both the broader Australian economy as well as in the procurement and use of IoT devices across the Government.

Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?

Palo Alto Networks supports the adoption of international standards, and we welcome the Australian Government's interest in ESTI EN 303 645 as an appropriate standard for smart devices.

Governments must draw on existing industry-led, globally harmonised Information and Communication Technology (ICT) Standards. Unfortunately, some governments and multilateral organisations are increasingly seeking to develop ICT standards or promote country-specific / unique standards that companies must use. Policies like these, while often well-intentioned, can sometimes harm innovation and security, largely because they run counter to how the ICT industry works. The ICT industry can create leading-edge, sophisticated, affordable products because companies can build one product version that is sold globally, saving costs and raising manufacturing efficiencies. The ICT industry also builds to voluntary, global, industry-led consensus-based standards that are accepted (or chosen) by the marketplace as the most effective or most appropriate. Diverting resources to meet country-specific requirements negates these benefits because companies must build tailored products in addition to global product lines. This raises costs (ultimately to customers) and drains resources from research and development - and often leads to companies walking away from these cost-prohibitively expensive markets. Such discriminatory policies also likely decrease security - as countries with specific requirements are unable to access the best in market technologies (that might meet international standards but may not meet specific county requirements).

If the Government was looking to mandate standards of security in line with ESTI EN 303 645, we would recommend that only the top 3, or potentially top 5, requirements be mandated. These are identified as the highest priority to achieve the greatest security benefit, while also noting the complexity and cost associated with implementing all standards as articulated in ESTI EN 303 645.

Chapter 7: Labelling for Smart Devices

> What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Palo Alto Networks notes the importance of consumer education on cyber security and cyber threats. For these reasons we continue to recommend that the Government launch a large-scale, national awareness campaign about cyber security and how people can protect themselves against cybercrime (see below at question 28) . This will ensure that consumers are more informed about the risks presented by their IoT devices when they are purchasing them. We also understand the Government's desire to provide some standardised way for companies to communicate with the consumer regarding the level of security of their IoT device. However, we suggest that there may be merit in exploring some more dynamic ways to do this via digital labelling of IoT devices. This could include providing a link to a webpage where companies can articulate their alignment with the top 3 - 5 standards of ESTI EN 303 645. This would allow companies to dynamically update their alignment with these standards as new information comes to light.

Chapter 8: Responsible Disclosure Policies

> Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

This section explores the role of responsible disclosure policies to support software developers and businesses to identify and resolve vulnerabilities, and what Government can do to help. The paper notes that adoption of responsible disclosure policies among Australian businesses remains low, although "responsible disclosure policies are increasingly being adopted by businesses and governments in international markets." The report suggests the Government could promote voluntary approaches to increasing responsible disclosure by releasing guidance or tool-kits for industry on the process of developing and implementing responsible disclosure policies. The Government could also regulate in this space, by considering “driving adoption of responsible disclosure policies through existing regulatory frameworks.”

Responsible vulnerability disclosure- or coordinated vulnerability disclosure as it is widely known- is a very important practice allowing the security community to give vendors an opportunity to fix vulnerabilities before releasing information publicly.

The Government should mandate the use of coordinated vulnerability disclosure and management policies that reference/align with existing international standards for vulnerability disclosure (ISO/IEC 29147) and management (ISO/IEC 30111). These standards, developed over years through international collaboration, lay out best practices for validating, prioritising, and remediating reported vulnerabilities so that all known vulnerabilities can be addressed in a coherent and efficient manner, while carefully considering the nuances of vulnerability handling and disclosure. If Australia promotes or mandates that businesses establish coordinated vulnerability disclosure and management policies that deviate from these ISO standards without consideration for the delicate nature of vulnerability disclosure and associated risks, they risk re-inventing standards that have matured and perfected over years. This will duplicate efforts, reduce the overall consistency in the application of standards across the world, and ultimately impact Australia’s security posture.

Chapter 10: Clear Legal Remedies for Consumers

What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

Palo Alto Networks encourages Treasury’s review into the application of Australian Consumer Law (ACL) of digital products to account for unique aspects which affect cyber security goods and services. These include but are not limited to a) the rapid and evolving threat landscape - which can mean that, through no fault of the business/manufacturer, a device that is relatively secure one day, may not be secure against a brand new cyber attack the next day; and b) human error is often the cause of security breaches (for example failing to patch or misconfiguration, etc). These factors are unique when compared to traditional goods and services that may be covered by the ACL.

Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

Palo Alto Networks encourages individuals to use existing tools and exercise individual rights in the Privacy Act via the Office of the Australian Information Commissioner (OAIC). Palo Alto

Networks cautions against a potential addition of "direct right of action", which could lead to frivolous actions and predatory lawsuits (e.g., where lawyers actively pursue clients whose [privacy] rights have allegedly been breached). This type of redress may also have an indirect consequence of being discriminatory against those who are not tech/security-savvy to recognize that a company breached their trust by not employing sufficient security standards - in other words, it may place too much of a burden on the individual. Evidence shows that litigation is not a great tool for policy making. If advancing public interest is of primary concern, the Government may consider removing enforcement of financial incentives entirely and requiring injunctions or equitable relief from the company at-hand. A right of direct action may cause undue burden and be counterproductive for businesses who will be forced to deal with these actions.

Other Issues

> What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?

We note our recommendations under "General Comments" and in particular underscore the need for the Government to incentivise Telcos/ISPs to adopt a clean pipes policy that sees malicious traffic detected and blocked in real time as it traverses the network. This will provide protection at scale to businesses and individuals across Australia.

We would also recommend that the Government launch a large-scale, national awareness campaign about cyber security and how people can protect themselves against cybercrime. Australia has a history of large-scale, national campaigns aimed at educating 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 develop and launch a nationwide campaign to help Australians understand cyber security and cybercrime, and basic steps they should take to protect themselves. This campaign could deliver a simple message like "Lock It Up, Back It Up, Patch It Up" and should be delivered in partnership with the private sector. This would help raise the profile of cyber security and its importance across the economy.

About Palo Alto Networks

Palo Alto Networks, the global cyber security leader, is shaping the cloud-centric future with technology that is transforming the way people and organisations operate. Our mission is to be the cyber security partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

Palo Alto Networks is committed to helping Australian Governments and private organisations across all industry sectors embrace the digital world safely and protect their business operations from cyberattacks. Many of our customers are Australia's largest enterprises and government organisations. We also have undertaken a range of activities that contribute to strengthening Australia's cyber security posture, including hosting roundtables with government and enterprise stakeholders to promote thought leadership; and partnering with the education sector to design cyber security courses. For more information see https://www.paloaltonetworks.com.au/