Australian Government
Department of Home Affairs
3 Lonsdale Street
Braddon
ACT 2612

1 November 2019

RE: Call for Views on Australia's 2020 Cyber Security Strategy

Palo Alto Networks appreciates the opportunity to comment on the Call for Views on Australia's 2020 Cyber Security Strategy. We support Australia's commitment to cybersecurity. Australia understands that cybersecurity underpins the country's economy and national security and is essential to maintaining the trust and confidence of its businesses and citizens in the digital age. Australia's landmark 2016 Cyber Security Strategy has been a catalyst for change, launching a series of government and private sector activities and responses to cybersecurity and cybercrime challenges such as opening the Australia Cyber Security Centre; establishing Joint Cyber Security Centres in five cities; and investing in skills and education. Australia also is taking a global leadership role via its International Cyber Engagement Strategy, which spearheads comprehensive and coordinated engagement on international cyber affairs to reduce the risk of cybercrime, foster good cybersecurity practices, and promote peace and stability in cyberspace.

Of course, threats will continue to proliferate, affecting Australian citizens, business, and government at the state, territory and national levels. We agree wholeheartedly with the assessment in the consultation regarding the growth and scale of malicious cyberattacks. The plan to update Australia's Cyber Security Strategy recognises the dynamic nature of cyber threats and underscores Australia's commitment to further adapt and implement national policy responses to tackle cybercrime and meet the country's evolving cybersecurity needs.

We approach this consultation by recommending key actions government can take to improve cybersecurity throughout the Australian economy. Our recommendations are derived from lessons learned and best practices from our collective experience at Palo Alto Networks, with operations in over 150 countries, working with governments around the world including the US, Australian, UK, and other governments.

1. Operationalise Concrete Public-Private Partnerships

We agree with the Australian government's long-standing position that public-private partnerships are essential to improving cybersecurity. Regular interaction and consultation between the cybersecurity community and government bring myriad benefits on both an operational and policy level. In its 2020 strategy, Australia should take the opportunity to make this concept more concrete and relevant to today's dynamic rates of change in cyberthreats, technology, and business models. To that end, we suggest establishing new structures to allow the Australian public and private sectors to interact in an ongoing, consistent, and practical way to share ideas, new developments, and other information in order to be able to quickly act and change course as needed when circumstances change.

- **Create an initiative allowing private-sector cybersecurity experts to work in the Australian Cyber Security Centre (ACSC) on a part-time basis to exchange knowledge and insights**

To more effectively collaborate on an operational level to address real-world cybersecurity challenges, Australia should look to establish a program in which private-sector experts can work alongside ACSC experts.

The UK has a similar initiative, the Industry 100 (or i100), set up by the National Cyber Security Centre (NCSC) in 2016.[1] Under the i100, private-sector cybersecurity experts join the NCSC on a temporary basis to bolster collaborative work between NSCS staff and industry personnel. Roles typically involve industry experts, such as threat researchers, coming to work part-time (e.g. fortnightly) within NCSC teams; roles also can include bespoke projects.[2]

This approach accords numerous benefits to government, industry, and cybersecurity generally. Government and industry experts jointly work on real world, current cybersecurity threats and challenges, allowing all parties to collaborate to investigate threats, learn lessons, identify systemic vulnerabilities, and reduce the future impact of cyberattacks. Government benefits from leveraging the collective brainpower of industry. Industry can support the government and their country operationally without it being overtly impactful on their staff's day jobs. Industry can also build their peer and governmental networks, as well as gain insight into government process.

While the UK's i100 is still in its relatively early days, the program has shown value. For example, i100 has held day-long workshops focused on one threat or actor. Declassified intelligence is provided to i100 members who enrich it with their own data, collaborate, and investigate. The outcomes include holistic reports focusing on specific threats/actors or sectors, providing an improved view of the landscape and indicating immediate actions to improve organisations' security postures. Both the NCSC and industry benefit. The NCSC typically gains many more leads and data points, allowing for further analysis. Depending on the nature or the traffic light protocol (TLP) rating of the information, industry many times can enrich its data

[1] https://www.ncsc.gov.uk/information/industry-100

[2] In the UK's model, companies are expected to continue to pay salaries for secondees to ensure that secondees maintain their independence and can provide a constructive challenge whilst in the role. Source: i100 website.

with the findings from joint initiatives to in turn help its research and customers. In short, this is a mutually beneficial model that allows for scalability and gives a balanced quid-pro-quo.

- **Establish industry consultation body/bodies to advise government officials on cybersecurity on an ongoing basis**

We also recommend establishing an industry consultative body or bodies to advise/ support the government's activities (and by extension efforts of critical infrastructure and enterprises in Australia). These consultative bodies should include leading industry officials with experience, expertise, and equities in cybersecurity. Some specific suggestions are:

- A group consisting of cybersecurity companies as well as businesses from various sectors, such as finance, telecom, energy, and other critical infrastructures, all of which deal with cybersecurity challenges daily. This should include large and small as well as domestic and international firms.
- Structured government-industry partnerships aligned with Australia's critical infrastructure sectors. A similar approach has been taken in the United States via the Sector Coordinating Council (SCC) framework.[3] SCCs are self-organised and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SCCs coordinate and collaborate with U.S. government sector-specific agencies (SSAs) and related Government Coordinating Councils (GCCs) to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.
- Bodies focused on gathering and sharing cyber threats, such as malicious/known attacks. Standing information sharing groups are often sectoral-specific, such as Information Sharing and Analysis Centers (ISACS) or can follow the ACSC/JCSC models which are more like threat intelligence hubs for federal and provincial government as well as critical infrastructure companies. An example again is the United States, which since 2015 has sought to encourage a wider range of participation in threat sharing by promoting Information Sharing and Analysis Organizations (ISAOs), which may form around a specific threat, such as countering botnets, or across industries.

[3] https://www.dhs.gov/cisa/sector-coordinating-councils

2. Take Measures to Improve Safety and Security of Mobile/ Internet Connections Throughout the Australian Economy

In updating its Cyber Security Strategy, Australia has made clear it wants to be prepared to address significant cybersecurity challenges on the horizon. The Internet of Things (IoT – including its consumer, corporate/enterprise, and operational/industrial [IIoT] applications) and 5G will open new areas of cybersecurity risk that need to be protected. Australia has already established international leadership in its initial approach to 5G and supply chain issues. As more entities and citizens continue to connect IoT devices and leverage 5G, the attack surface will grow. Australia's 5G and IoT networks will need to continually demonstrate a high level of safety and security, and thus both deserve attention in the 2020 Cyber Security Strategy. Otherwise, bad actors – including nation states – will be in a better position to infiltrate networks and gain access to and control of information and devices connected to them.

5G

Australia is embarking on its 5G buildout, with the Australian Communications and Media Authority (ACMA) issuing 5G licenses to service providers as well as private enterprises building their own 5G networks. As Australia rolls out 5G, ensuring 5G networks are secure and trusted by design should be a priority.[4]This approach can help to avoid some of the challenges we have securing today's 3G and 4G networks, which arguably were not architected to be secure by design. As Australia moves closer to a digitally connected 5G world, there are an increasing array of attack vectors – inside out, outside in, and roaming, to mention just a few. Infected "trusted" end devices become sources of inside-out attacks, targeting external web sites, creating signaling storms, wasting bandwidth, and stealing data from users and providers. Furthermore, mobile and fixed line networks infrastructures' convergence can result in unsecure interconnectivity points, which need to be protected. Secure Wi-Fi and LTE access and handover challenges are additional problems. The threat and potential damage is relevant not just to Australia's telecom/service provider sector, but to the many interconnected sectors including energy, finance, healthcare, transportation, IT, government, manufacturing, and retail. Given all of these challenges, 4/5G infrastructure security requires a holistic approach, where prevention is the key ingredient to the infrastructure.

[4] Australia has taken important steps to ensure the security and resilience of Australia's telecommunications infrastructure, notably via the Telecommunications Sector Security Reforms (TSSR) of September 2018. The TSSR require covered entities to do their best to protect networks and facilities from unauthorised access and interference – including a requirement to maintain 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by them. Supervising and controlling networks and facilities should be complemented by other efforts.

Australia should:

- **Encourage telecommunication and internet service providers to have complete visibility of threats on their networks**

Cybersecurity threats (malware, viruses, command-and-control, others) regularly traverse mobile networks. Cybercriminals continue to introduce and update new attack tools, such as using automation and exploit toolkits, leveraging the cloud, attacking mobile operators' infrastructure, communication tunnels, and also their end users (consumers and enterprises). Networks are a vantage point leveraged by attackers, and until we improve our ability to detect and prevent threats passing through these networks, the volume of attacks will only increase.

To address threats running across networks, government should play an active role in ensuring that it can reduce the amount of high volume, low sophistication threats entering Australia. As the threat is not only limited to pending rollouts of 5G networks, the Australian Government should encourage any entities with a 4G license as well as internet service providers to have complete visibility of their networks in order to take steps to detect and prevent cyberattacks in real time. This can complement the use of proper end–to-end encryption (IPSEC). IPSEC should be expected on critical segments of the network, as it provides security against tampering of data travelling through the network. However, IPSEC does not provide visibility into whether the encrypted traffic passing through the encrypted tunnel is malicious or not.

- **Encourage 5G operators to design into their networks a high reliance on automation, machine learning, and artificial intelligence (AI)**

5G operators need to design their infrastructure with security technology implemented that will accommodate and handle high-volume traffic, with automated orchestration and response, allied with an ability to reliably identify and report on specific targeted attacks. 5G will require a dense network of small cell-based stations managing high-volume, high-speed traffic across complex network slices. To achieve proper fault management and resiliency, prospective 5G operators should be expected to design into their networks a high reliance on automation, machine learning, and AI. Cybersecurity technology and management choices made by operators should reflect this reliance and be fit for purpose to manage risks associated with this approach.

- **Promote a Zero-Trust approach**

Australia's revised Cyber Security Strategy should promote a Zero Trust architecture that is rooted in the principle of "never trust, always verify". Under the Zero Trust concept, an organisation should not automatically trust any unauthenticated activity inside or outside its network perimeters. Instead, an organisation must authenticate anything and everything trying to connect to its systems before granting access. That level of granular control around key critical infrastructure and data allows for management of cyber risk much more effectively. We recommend Zero Trust as a best practice for operators to effectively secure a 4G environment that is IP end-to-end which then allows a safe and secure transition to a 5G environment, where an open standards-based architecture will dominate.

IoT

- **Promote IoT security at both the network and device level**

Australia clearly understands the cybersecurity risks resulting from IoT proliferation. Government should approach this issue first and foremost at the network level as well as the device level. We stress the network level as a priority because IoT device security, while important, is often a very operationally inefficient approach 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).

Network level: The network is a logical detection and enforcement point for IoT security. 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 optimize their connected devices. Furthermore, applying a 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, such as by establishing a public-private sector working group with a year's mandate to develop recommendations. 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.

Device level: In addition, the government should look to implement regulatory steps to ensure that devices sold into Australia meet minimum baseline security requirements. A useful baseline could be to disallow product shipments that have some if not all the vulnerabilities listed in the OWASP Top 10 Internet of Things Vulnerabilities:[5] weak, predictable, and hard-coded passwords; insecure network services; insecure ecosystem interfaces; lack of secure update mechanisms; use of insecure or outdated components; insufficient privacy protections; insecure data transfer and storage; and lack of device management. These have been the most prevalent vulnerabilities for IoT for some time now, and by focusing on discouraging the shipment of devices with these issues, Australia can go a long way toward stemming the flow of vulnerable devices connected to Australian networks.

[5] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

3. Take Additional Measures Related to Awareness and Education, and Skills Development

- **Launch a large-scale, national awareness campaign about cybersecurity 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. Cybersecurity, 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 cybersecurity and cybercrime, and basic steps they should take to protect themselves.

- **Leverage a standardised framework for categorising cybersecurity work**

Page 13 of the consultation paper states: *Access to skilled professionals is an important part of a 'trusted market'. Government continues to receive feedback about a cyber security skills gap in Australia...Some stakeholders also have raised concerns about whether the education and training system is meeting the needs of the cyber security sector, and whether sufficient data is available on this issue. Part of the problem could be confusion about what qualifications are needed for what cyber security jobs.*

To address the gap between qualifications and jobs, the government should drive the creation and use of a standardised framework to categorise and describe cybersecurity work that could be used by academic institutions and vendors to standardise their curricula and certification, and employees and employers to best match needed job skills. A helpful example is the National Initiative for Cybersecurity Education (NICE)'s Cybersecurity Workforce Framework issued in August 2017 by the National Institute for Standards and Technology (NIST) in the United States. The NICE framework (*NIST Special Publication 800-181*) establishes a taxonomy and common lexicon to describe all cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework is comprised of categories, specialty areas, and work roles; the latter lists the knowledge, skills, and abilities requires to perform tasks in a given role. The NICE Framework serves several key constituents within the cybersecurity community, including employers, current and future cybersecurity workers, staffing specialists and guidance counsellors, training and certification providers, education providers (many of which currently develop unique curricula), and technology providers.

A similar standardised framework in Australia would be particularly helpful in supporting skills development and hiring. We understand that AustCyber has been a proponent of using the NICE

Framework in Australia, and Palo Alto Networks would be eager to support their effort by contributing our experience and expertise working with the NICE Framework with over 600 colleges and universities in 70 different countries.

4. Recommendations in Response to the Consultation's Questions About Legislation

Page 12 of the consultation states: *As the risks and consequences from malicious cyber activity rise, we are seeking your feedback about whether Government's approach to cyber security laws needs to change. Both stronger enforcement of existing laws and new requirements could be considered. If change is needed, Government would favour the option that delivers the largest long-term benefits for society while minimising any upfront costs for industry.* It further states *Both stronger enforcement of existing laws and new requirements could be considered.*

We have two suggestions related to the questions on legislation.

- **Consider the EU NIS Directive as a model for risk-based cybersecurity legislation**

Pages 11-12 state that *"A better approach may be consistent but flexible cyber security laws for critical systems"* and provide the EU's Network and Information Security (NIS) Directive as a case study to consider.

We agree the NIS Directive could be a model for Australia. As noted in the consultation, the NIS Directive establishes security and incident notification requirements for covered organisations. Organisations must have "regard to the state of the art technologies" to manage risks posed to the security of the networks and information systems used to provide the covered services, and also must take appropriate measures to prevent and minimise the impact of incidents. Security incidents of certain magnitudes must be reported to national competent authorities. These obligations apply whether the covered companies manage their own network and information systems or outsource them.

The strengths of the NIS Directive are:

1. It directs organisations to have regard for the state of the art technologies. Cyberattacks are constantly evolving, sophisticated, automated, and rising in volume. As such, state of the art technologies --- such as those that evolve accordingly, leverage automation, and that secure information whether in the network, on endpoints, or in the cloud—are imperative.
2. It stresses prevention. Preventing successful cyberattacks is part of a holistic approach to cybersecurity risk management. While detection, response to and recovery from incidents are important, at that stage the damage is done in terms of lost intellectual property, customer and personal data, damaged reputation, impacted systems, and lost customer

trust. Given the rise in volume and sophistication of attacks with never-before-seen malware, a focus on preventing successful attacks is needed.

3. It is not overly prescriptive/ does not mandate a particular technology. The Directive instead directs covered organisations to understand and manage their risks. This approach is key because cyberthreats are constantly evolving and the risks to each organisation are unique, based on the particular information and systems they need to protect.

If Australia goes down a similar path as the NIS Directive, we recommend it do the following:

1. Provide resources and guidance for covered organisations and government. A good example is the UK government, which has issued guidance on the NIS Directive aimed at covered organisations, including some sector-specific guidance (such as for the healthcare sector). The UK government also provided guidance documents to be used by government agencies charged with implementing the Directive for sectors they oversee and assigned the UK National Cyber Security Centre (a non-regulatory body) to be a technical resource to these agencies.
2. Provide organisations guidance on how to validate their efforts. Effective implementation of any cybersecurity law must be ongoing as companies work to implement it and raise their cybersecurity postures. If Australia issues a law similar to the NIS Directive, it should consider providing ongoing guidance and expertise to organisations about metrics of effective cybersecurity and how to validate their efforts. Cybersecurity risk management is an ongoing process, and useful lessons will continue to be learned.

- **Explore ways to leverage Australia's personal data breach notification requirements to help all organisations improve their cybersecurity**

Australia currently requires that certain personal data breaches be notified to the Office of the Australian Information Commissioner.[6] Australia should study whether select information about breaches—namely the tactics or techniques employed—could be anonymized and leveraged to allow other organisations to protect themselves. For example, anonymised or redacted cases could be available for any organisations to consult to see if they might be susceptible to similar issues and to proactively protect their environments.

5. Improve the Australian Government's Cybersecurity Posture

Government should take concrete steps to improve its own cybersecurity posture. Efforts in this regard will help government better protect government and citizen data and offer online citizen services, while also providing a role model to other sectors of the Australian economy. To this end, we recommend the following:

[6] https://www.oaic.gov.au/privacy/notifiable-data-breaches/

- **Improve government procurement and utilization of cybersecurity technologies**

With the threat landscape changing daily we need to ensure that, where possible, agencies must be able to procure and leverage technologies at a faster pace. Three recommendations follow.

First, accelerate a safe and secure move to the cloud. Like many governments, Australia would like to move to the cloud. Consuming cybersecurity protections as a service (e.g. via the cloud) will allow the Australian government to adapt more quickly to evolving threats. However, there is hesitation about how to move to the cloud safely and securely. There are steps government can take to ensure a move to the cloud is safe and secure. Government also should look to streamline the way an agency can procure cloud services by reducing the time it takes to certify cloud products on the cloud panel (Australia's marketplace to procure approved cloud services). One idea is to consider leveraging approaches in the other "Five Eyes" countries to certify the use and adoption of cloud services, such as the U.S. FedRAMP experience (see below).

Second, update Australia's certification frameworks for public procurements to make them risk-based and globally compatible. Whilst the Australian government is looking to review the process around IRAP assessments and the ACE program, it should consider the following:

1. *Adopt a risk-based model.* Rather than a compliance-based approach, thoughts should be given to using a risk-based model with guidelines so that providers can assure how they mitigate risks the government deem as critical. We suggest moving away from the current IRAP assessment which is predominantly based solely on compliance.

2. *Consider alignment with, or even mutual recognition of, other Five Eyes country approaches.* This should also include identifying consistencies among what is allowed through agency threat and risk assessments, what is listed on the Evaluated Products list in Australia, and the Common Criteria. Mutual recognition will be helpful to agencies that need to access solutions as quickly as possible rather than waiting for something to be accredited locally.

   FedRAMP cloud procurement: An example of an approach that could be emulated is the U.S. Federal Risk and Authorization Management Program, or FedRAMP, a U.S. government-wide program that promotes the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment. FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government. FedRAMP's goals are to: 1) Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations; 2) Improve confidence in the security of cloud solutions and security assessments; 3) Achieve consistent security authorizations using a baseline set of agreed-upon standards for cloud product approval in or outside of FedRAMP; 4) Ensure consistent application of existing security practices; and 5) Increase automation and near real-time data for continuous monitoring.[7] Overall, this approach saves time, money, and effort for both federal government agencies and cloud service providers.

3. *Consider using third-party certifiers.* There is an ever-growing number of solutions that will need to be certified. The government should look to enlist other agencies or accredited third parties to do testing which meets government requirements. This would allow more solutions to be tested more quickly, allowing for greater access to approved solutions/ adoption of solutions by government agencies.

Third, promote the government's secure use of IoT. Our IoT recommendation above suggests focusing first on IoT security at the network level, and secondarily at the device level. This approach should be leveraged in the Australian government as it increasingly deploys IoT devices. Above we suggested launching a concerted effort to determine how to approach IoT security at the network level, such as by establishing a public-private sector working group with a year's mandate to develop recommendations. The government should prepare to leverage any outputs of such an effort.

- **Establish a government-industry supply chain security task force**

Australia is rightly focused on supply chain security, and the consultation covers this topic (Qs 12-13). Australia set an important precedent in its 5G policy by highlighting the supply chain concern of including suppliers who are subject to extrajudicial direction from other countries. This precedent should be considered in critical infrastructure beyond 5G. Additionally, Australia should consider the security implications of companies who share the source code of their unique intellectual property (IP) with governments as a condition of access to certain markets.

The government should consider how to create incentives for companies to adopt best practices in areas such as supply chain risk management. This is a very effective way to increase the level of trust in the security of the technology procured and employed to defend the government's information networks and critical mission systems. Government and private industry should work collaboratively to identify other supply chain best practices and develop a menu of potential incentives – such as qualified bidder lists – to promote their adoption.

An approach we recommend the Australian government take to enable some of these changes is to set up a government-industry supply chain task force similar to an approach in the United States. In 2018, the U.S. Department of Homeland Security established the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force to identify and develop consensus strategies that enhance ICT supply chain security in the United

[7] https://www.fedramp.gov/

States.[8] The joint government-industry task force is comprised of approximately 40 individuals representing the IT and telecommunications industries and 20 people from relevant government agencies (approximately 60 total). In addition to assembling an inventory of existing supply chain risk management efforts across government and industry, the Task Force launched four main work streams:

- Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry;
- Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services;
- Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s); and,
- Producing policy recommendations to incentivise the purchase of ICT from original manufacturers or authorized resellers.

In September 2019, the Task Force released an interim Report: “Status Update on Activities and Objectives of the Task Force.”[9] This Report details the Task Force’s methodologies, areas of discussion, and, where appropriate, key findings, recommendations, and potential areas for further study identified by each of the Task Force’s four constituent Working Groups, highlighting impacts of the Task Force’s overall mission on supply chain risk management. The findings and recommendations of the Working Groups will inform the Task Force’s second year of activity. In its next phase, the Task Force and the Working Groups will continue to support efforts by the U.S. Federal Government and industry to manage ICT supply chain risk.

Conclusion and About Palo Alto Networks

As the Australian government embarks on its 2020 Cyber Security Strategy, Palo Alto Networks is ready to contribute our expertise and experience to help ensure Australia is well equipped to employ cybersecurity as an enabling bedrock of modern, digital economic and public service delivery to maintain trust in the digital age. We would be happy to discuss our ideas further. For more information, please contact Sean Duca, vice president and chief security officer, Asia Pacific & Japan, at [redacted]

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be

[8] https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force

[9] https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf

the cybersecurity 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 the Australian government 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 cybersecurity posture, including hosting our first-ever 5G security event in Sydney in July 2019; hosting roundtables with government and enterprise stakeholders in Sydney and Canberra to promote diversity and address cybersecurity skills shortage; publishing our book 'Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Australia' with actionable insights and advice from key thought leaders from Australia's public and private sectors; and partnering with RMIT Online and Swinburne University to design cybersecurity courses. Further, five Australian institutions of higher learning are Palo Alto Networks Authorised Academy Centres (AAC) as part of our Cybersecurity Academy Programme.

For more information see https://www.paloaltonetworks.com.au/