24 June 2022

Digital and Technology Policy Division
Strategy and National Resilience Group
Department of Home Affairs
Canberra, ACT, 2600
(Submission Made Online)

RE: Call for Views on the National Data Security Action Plan

Palo Alto Networks appreciates the opportunity to provide a submission in response to the Government's call for views on the development of the National Data Security Action Plan (herein 'the Plan').

Palo Alto Networks is the global cyber security leader, securing the networks and information of 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 data and its willingness to engage stakeholders in the development of the Plan via a public consultation process.

General Comments

Distinguishing Between Content Data and Security Data

While the discussion paper acknowledges the varying levels of sensitivity and criticality across types of data in the development of the three data security pillars, Palo Alto Networks believes the Plan could benefit from additional detail that would clearly distinguish between content data and security (or system) data. This would acknowledge that the risks and policy approaches applied to these distinct types of data need to be different to ensure that the Plan can meet its objectives of securing Australian data.

Globally, conversations about data tend to focus on well-understood types of data - such as personal data or sensitive government data.[1] These types of data largely fall into a category of data called "content data". Content data refers to data whether in digital, optical, or other form that conveys essence, substance, information, meaning, purpose, intent, or intelligence. Governments may have legitimate reasons why they may want to store certain content data onshore. These decisions should be risk-based and restricted to certain types of content data.

[1] For example, the "Figure 1 – A simplified view of data movement" in the Data Security Action Plan focuses on the creation and storage of content data.

In contrast, security data (also known as systems data) is data relevant to or used for the purposes of, security research or enhancing security services or offerings. Security data includes device, network and endpoint information as well as other information such as to URLs/Domains, session data, threat intelligence or data, statistics, aggregated data, netflow data, "telemetry data", and in some limited cases, may include certain personal and content data where it is necessary for the furtherance of security (such as a hyperlink to a malicious website or a malicious IP address). Security data is central to an organisation's ability to protect against cyber threats. Laws or policies that restrict the cross-border flow of security data can deprive organisations of the benefits of real-time, globally deployed preventative defences and security, and of the ability to correlate information about cyber threats in real-time. Restrictions on the free flow of security data may also impact the development of artificial intelligence/machine learning (AI/ML) in a security context and how an organisation manages cyber security as an integrated risk across the enterprise. These concepts are explored below at Question 5.

Distinguishing between these different kinds of data, and recognising the importance of the free flow of security data across borders in real-time, will help ensure that Australians can continue to leverage digital technologies in a safe and secure manner. It will also ensure that Australia's policy and legislative approaches to data remain fit for purpose and do not unintentionally make Australia more vulnerable and susceptible to cyber attacks.

Key Questions

Call for Views

1. What do you consider are some of the international barriers to data security uplift?

The free flow of security data across borders is integral to our collective cyber defences. The continued and real-time sharing of security data is one of the best ways to uplift data security across the broader ecosystem. For more details, please above "General Comments" and below at Question 5

2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

We believe that Australia's data protection framework should generally align with the EU's GDPR. We provided this point of view in responding to the Attorney-General's Department in response to their call

for views on the Privacy Act Review - Issues Paper on 26 November 2020.[2] Australia's data protection and security framework should also include key tenets of the GDPR that relate to the importance of processing data for security purposes. Recital 49 of the GDPR recognises that ensuring network and information security is a "legitimate interest" of entities for processing personal data. EU legislators are currently working to embed this point even more clearly as they revise the 2016 cyber security law, the Network and Information Security Directive (the new name is "NIS2"), to include language reiterating this point. NIS2's final text (as of 17 June 2022) Recital 69 states *"The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by essential and important entities, could be considered legitimate to comply with legal obligation subject to the requirements of Article 6(1)(c) and (3) of Regulation (EU) 2016/679,*[3] *of the data controller concerned as referred to in Regulation (EU) 2016/679*). *Processing of personal data might also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of these entities, pursuant to Article 6(1)(f) of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information sharing arrangements or the voluntary notification of relevant information as laid down in this Directive. Measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools may require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses, time stamps – where those reveal personal data.."*

3. What additional guidance or support from the Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?

Palo Alto Networks would encourage the Australian Government to focus on uplifting the collective understanding - across both the public and private sector - of how data can be secured in the cloud, and address some of the common misconceptions about data localisation. This could be achieved via the delivery of guidance materials or via workshops but should target both technical and non-technical audiences across small to large organisations. We have explored these two key issues below (which may also be relevant to Question 14):

1) *Education Initiatives Centred on How to Secure Data - Beyond the Location of Data.*

[2] https://www.ag.gov.au/rights-and-protections/publications/submissions-received-review-privacy-act-1988-issues-paper

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (the General Data Protection Regulation (GDPR)).

We believe the Australian Government via the Australian Cyber Security Centre (ACSC) and the Department of Home Affairs (DHA), has a role to play in educating stakeholders on how their data can be secured in the cloud. This should be done in close partnership with Industry, which can inform, support, and amplify this messaging.

As with on-premises applications and data, those stored in the cloud must be just as vigilantly protected. While there are questions about whether data in the cloud is "less secure", the reality is there are a range of ways that cloud offerings are in fact more secure and provide users with better security features to secure their data in the cloud. The cloud offers many advanced security features (e.g. granular permissions and access management) that support secure data storage and handling. Cloud storage providers also implement baseline protections for their platforms and the data they process, such as authentication, access control, and encryption. From there, most enterprises supplement these protections with added security measures of their own to bolster cloud data protection and tighten access to sensitive information in the cloud. It is important to note that cloud security is a shared responsibility between the cloud service provider (CSPs) (who is responsible for securing the infrastructure) and the user (who is responsible for securing their data in the cloud).

Aside from the mechanisms listed above, there are numerous controls a user can put in place to further secure and protect their data in the cloud. This can include implementing Bring Your Own Key (BYOK) measures. BYOK capabilities are offered by most CSPs to provide individuals, governments, and organisations with additional measures to secure their data stored in the cloud. BYOK enables only those individuals and/or organisations who possess a "key" to decrypt their data stored in the cloud - this means that not even the CSP can see your data stored in the cloud. Some CSPs will also provide their Key Management System (KMS) so organisations can easily manage and deploy keys in their environment. CSP will also implement many layers of audit and protections to prevent unauthorised access to these keys. Implementing these measures can ensure the confidentiality of data stored in the cloud.

2) Addressing Misconceptions and Other Beliefs About Data Localisation

The ACSC is the technical advisory body for cyber security matters in Australia. Businesses of all sizes look to the ACSC for technical advice and guidance. As such, Palo Alto Networks would encourage the ACSC and the DHA to engage with stakeholders from academia, the private sector and civil society to look at the complex issues and misconceptions surrounding data localisation. Below are some suggested areas to the Government may wish to address and explore:

A. Misconception: Data Localisation Improves Data Security

The security of data depends primarily on the logical and physical controls used to protect it, such as strong encryption on devices, perimeter security for data centres and how well data is segmented and access is controlled. Provided that the data does not reside in a jurisdiction subject to extrajudicial control or interference by a foreign entity, the nationality of who owns or

controls servers, or the location of the servers, has little to do with data security.[4] Data security depends on the implementation of technical, physical, and administrative controls, which can be strong or weak, regardless of where the data is stored. To ensure the security of data, priority should be given to measures that can contribute to good cyber security, such as adopting Zero Trust Architecture, rather than a focus on data location.

B. Misconception: Data Localisation is Better for Privacy

While data localisation policies are sometimes justified by a stated desire to improve data privacy and protect individuals' data, by decreasing cyber security such policies can have the opposite effect.[5] Privacy policies are worth very little if cyber adversaries can compromise networks and access and exfiltrate personal data. Data privacy is improved by an organisation's commitment to balance all privacy considerations and collect, secure and use data in alignment with consumer and regulatory expectations, regardless of where the data is physically located. In short, securing personal data helps improve privacy.

C. Other Beliefs: Economic Cyber Sovereignty

Some data localisation policies are portrayed as a way to help countries "take back control" and create "sovereignty" from foreign firms and trading partners. This assertion can neglect that a complex interplay of economic, governance, social, and political factors determines a country's international competitiveness and approach to digital issues. There are ways to facilitate local economic growth outside the maintenance and localisation of data in the jurisdiction, such as making long-term investments in education, infrastructure, and other enabling factors that help local technology and cyber firms become more internationally competitive.

D. Other Beliefs: Macro-Economic Impact

The free flow of data is key to the health of the modern global economy, delivering countless benefits and enabling access to knowledge and tools around the world.[6] While data localisation might provide short-term commercial benefits to domestic firms, it may do so at the expense of innovation and long-lasting global economic growth.[7] Specifically data localisation may:

---

[4] N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them'. Available: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[5] N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them'. Available: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[6] A McKinsey Global Institute estimated that cross- border data flows contributed nearly $2.8 trillion to the global economy in 2014 through its enablement of the flow of goods, services, and other resources. The reports estimate that this figure could reach $11 trillion by 2025. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-executive-summary.pdf

[7] E Wu, 'Sovereignty and Data Localisation', Harvard Kennedy Belfer Center, Available: https://www.belfercenter.org/publication/sovereignty-and-data-localization

- Hurt local economies by increasing prices and limiting the availability of ICT products and services. This may inadvertently force local businesses to use less resilient or inferior services.[8]
- Suppress entrepreneurial activity and innovation.[9] Investments in start-ups and innovation more broadly, is typically based on having a large international market for such services. If there is substantial and widespread data localisation, investors will face a smaller expected market for any given innovation.[10]
- Deter companies from investing in a given country as mandating local storage of data vastly increases the cost of doing business for all companies.[11] This may adversely impact smaller countries that 'may not be large enough to support even one world-class data centre, much less provide the economic rationale for multiple data centres, which can cost a billion dollars or more.'[12]

Rather than benefiting the economy, measures that restrict data flows may have detrimental consequences for global and domestic economic development.

E. Other Beliefs: Jurisdictional Control

There can be a mistaken belief that firms can avoid oversight and requests for data by simply transferring data out of a country.[13] However, data localisation requirements do not change who is responsible for the data, regardless of where it is stored. According to the ITIF, 'organisations cannot escape from complying with a nation's laws by transferring data abroad' and consequently 'data localization is not necessary to force an organisation to comply with domestic data laws'.[14] For example, most national data breach requirements apply to businesses or organisations irrespective of whether the data breach occurs domestically or abroad. The transferring of data abroad does not mean that organisations can circumvent data protection requirements — as most companies doing business in a nation, including all domestic companies and most foreign ones, have a "legal nexus," which puts them in that country's jurisdiction.[15] Further, there oftentimes may be contract requirements that hold businesses and organisations accountable for how they use data.

F. Other Beliefs: Law Enforcement Access to Investigative Data

[8] A report by the Leviathan Security Group 'Quantifying the Cost of Forced Localization' estimates that efficiency losses from data localization measures can increase the costs of data hosting by 30-60%.
[9] According to the Center for Strategic International Studies (CSIS) Paper (above n5), data localisation policies may risk stifling competition, innovation and trade which provide better services for customers and can weaken data security.
[10] P Swire and D Kennedy-Mayo, 'The Effects of Data Localization on Cybersecurity', Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.
[11] As highlighted by 'Sovereignty and Data Localisation', PayPal suspended its Turkish operations in response to a requirement that PayPal fully localise its information systems within Turkey.
[12] P Swire and D Kennedy-Mayo, 'The Effects of Data Localization on Cybersecurity', Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.
[13] N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them'. Available: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.
[14] Ibid.
[15] Ibid.

Concerns about law enforcement access to data can be used to justify data localisation (the belief that data localisation is the only way to get local and foreign firms to respond to law enforcement requests). However, this fails to recognise the transnational nature of crime - particularly cybercrime. Cybercrime continues to pose a significant threat to the security and prosperity of governments, businesses, and citizens around the world. The Internet has made it easier for criminals to commit crimes online and across borders with relative impunity - enabling them to mask both their identity and location. Cybercrime traverses traditional nation-state boundaries - with victims and perpetrators frequently located in multiple jurisdictions (particularly where incidents are global in nature). As a result, combating cybercrime often relies on strong cyber threat intelligence sharing, as well as international cooperation and mutual assistance across the law enforcement agencies of numerous countries. In summary, the ability of law enforcement to combat cybercrime and other transnational crime types will be intrinsically linked to their ability to more easily share data with other countries. As such, data localisation can serve to handcuff investigators when seeking to disrupt or prosecute cyber criminals.

G. Other Beliefs: Security of Certain Government Data

As with the security of all data - government data or otherwise - it is more important to focus on the logical and physical security controls that comprise a multifaceted risk-based cyber strategy, rather than solely focusing on the geographical location of data. Over the last decade, we have seen cyber security breaches of both on-premise and “air-gapped” environments illustrating this point. While there may be a case that the free flow of government data to, or the storage of sensitive government data in, another country’s borders could threaten national security, there are a range of cyber security measures that can be taken to secure the data and restrict unauthorised third parties’ access (see above at Point 1). In addition, not all types of government data are the same, and policies can inadvertently broadly capture non-government data (e.g. security data).

H. Other Beliefs: Other National Security

Data localisation mandates affect a variety of national security interests - including the ability of security actors to share information, promote cyber security (please see the above section for more on this) and promote a free and open internet. Specifically, data localisation can limit collaboration between military, law enforcement, intelligence, and other security actors by creating obstacles to accessing data across borders. For example, the adoption of hard data localisation policies could jeopardise the information-sharing relationships among many allied and like-minded countries.

We are aware that the ACSC has released Cloud Security Guidance. These materials could be expanded in collaboration with industry and promoted across the public and private sector - including with senior

executives and non-technical audiences who may not be familiar with these issues but increasingly need a degree of familiarity with these matters.

4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market? a. What obligations are you most commonly subjected to from international jurisdictions?

We support the Australian Government's efforts to seek an adequacy decision with the EU. Adequacy would be beneficial, as this would afford an additional mechanism for companies to transfer personal data from the European Economic Area (EEA) to Australia, and make it easier for customers and service providers to transfer data aside from relying on other mechanisms, such as binding corporate rules, or standard contractual clauses. Palo Alto Networks notes that the ability to transfer data across borders is key to cyber security. Threats are global, as are our business and our customers' business, and we need to ensure that data can flow freely across borders.

5. Does Australia need an explicit approach to data localisation?

We would encourage the Australian Government to pursue policies and approaches that promote the free flow of security data across borders (as defined above). The free flow of security data across nation-state borders is integral to cyber security.

In today's world, cyberattacks are increasingly sophisticated and automated, launched by adversaries anywhere in the world, hitting targets in all countries. Governments, businesses and citizens are being systematically targeted by threats that may or may not originate from inside the country in which they reside.

To counter this, leading organisations in the cyber security community regularly leverage security data in which cyber threat information is combined from around the world to develop a global picture of cyber adversaries—their techniques, tactics, infrastructure, motives, and the like. To be most effective, security data must be made as accessible as possible across the globe, combining security and cyber threat information from as many countries as possible. In short, effective cyber security requires connecting the dots between different threats and taking immediate action to automatically deploy defences against these threats. In addition, because the threats can originate from, and target anywhere in the world, security data needs to be freely transferred in real-time between countries to best understand and counter the full range of cyber adversaries and threats we all face.

Restrictions on the free flow of security data across borders may impact the ability for the cyber security industry to share research, identify threats and develop migitations to protect governments, businesses, and individuals around the world from the attack. Mandates that security data remain onshore can also impact incident response, the ability for organisations to manage cyber security in an integrated way, and the development of AI/ML capabilities in the security context. The impacts of restricting the free flow of security data in real-time are explored in more detail below:

1) Impacts to Cyber Security Prevention Activities

The globally sourced analysis described above is regularly used to develop new protections such as automated preventive measures, which are deployed to customers globally to help them to prevent successful cyberattacks. In other words, the global model enables rapid response time to detect and prevent new and unknown threats (or threats similar to previous attacks) from impacting multiple organisations around the world. All organisations seeking to secure their networks and information - including governments, businesses, and consumers - across the economy benefit from a globally aggregated view of cyber security threats and a real-time global deployment of responses. If countries prevent security data from leaving their borders, valuable threat information will not be analysed as part of this larger effort, which means the cyber security community then may not be able to develop preventive measures as robust or effective as it otherwise could. It may also restrict the ability of an impacted country to warn others of an inbound cyber attack and may impact attribution efforts.

2) Impacts to Follow the Sun Services/Global Security Operations Centres (SOCs)

This global model of real-time transfer of security data is frequently used in the context of cyber security operations centres (SOCs) to ensure that cyber incidents can be identified, responded to and remediated as soon as possible, in an automated fashion/in real-time. This is increasingly important in the context of a global cyber security skills shortage - as it allows for the pooling of finite and highly-sought-after cyber security talent (i.e malware reverse engineers) who may only be located in one geography, to focus on more complex cyber security incidents - attacks that cannot be addressed by automation and require human intervention. Data localisation directly impacts this model as it would restrict the data that could be shared between these geographical sites - severely restricting the ability of global SOCs to detect, prevent and respond to cyber threats in real-time.

3) Impacts to Machine Learning and Artificial Intelligence (ML/AI) in the Security Context

Data localisation policies that restrict the free and real-time transfer of security data may adversely impact the development of AI/ML tools, which are increasingly important in combating cyber attacks.

Today, both cyberattacks and cyber security defences are leveraging automation.[16] To successfully protect against automated attacks, it is essential to fight fire with fire – or in this case, machine with

[16] An automated attack is one performed by a computer program rather than the attacker manually performing the steps in the attack sequence. While cyber adversaries have leveraged attack tools for quite some time, older tools could only initiate one attack sequence at a time, requiring human intervention to launch additional attack sequences. However, newer tools can perform the entire attack process automatically, and are creating unique malware at the rate of tens of millions per day.

machine – by incorporating automation into cyber security defences. Automation levels the playing field reduces the volume of threats and allows for faster prevention of new and previously unknown threats.

Automation is better facilitated by AI/ML. Whereas previously a human expert could classify a malicious sample, now we need AI/ML to automate this process at scale. While true automation should also be viewed as a tool that can, and should, be used to better predict behaviours and execute protections faster - if implemented appropriately and with the right tools, automation and AI/ML can aid in the prevention of successful cyberattacks.

However, all of these efforts may be thwarted by data localisation policies. Advanced and accurate AI/ML technology rely on high-quality, diverse and readily accessible datasets. As AI/ML "learns" from data, the wider and more diverse the data is, the more relevant the AI/ML technology can be. If the security data that AI/ML can access is restricted by jurisdiction, the AI/ML technology will develop bias and ultimately may not be as effective in detecting and preventing cyber attacks. This could have devastating impacts on the future of the cyber security industry and our collective cyber defences.[17]

4) Impacts on Cyberthreat Research

Cross-border data flows also are important to cyber security researchers, who gather, research, analyse, and provide insights into the latest cyberthreats. Cyber security researchers often collaborate across borders on their work, which for leading cyber security companies manifests not just in improved products to protect customers, but also in technical threat reports that can be shared with computer emergency response teams (CERTs) and other network defenders who use this research to harden their defences accordingly - feeding into the preventive measures (as described earlier). Prohibitions on the transfer of security data would hinder the effectiveness of this threat research and cyber threat information sharing. Given that cyber adversaries regularly share information/data across national borders about attack methods and victims, it is imperative that cyber defenders can share threat information in real time to raise our collective global defences.

[17] The ingestion and analysis of data required for AI/ML can occur in a manner consistent with privacy values and principles. AI/ML uses metadata and features extracted from the original data to make decisions about the maliciousness of the data. Techniques such as "differential privacy" ensure that when AI/ML feature data is extracted from personal and/or private data, it is safe to transmit outside an organisation, and the feature data mathematically cannot be later converted back into the original data.Indeed, when properly implemented, automated AI/ML can be more private than having a security expert review the raw data - the AI can be trained on the privatised data.

Case Study: WannaCry - Solved by Leveraging Global Data

On Friday, May 12, 2017, a series of broad attacks began that spread the latest version of the WanaCrypt ransomware. These attacks, also referred to as WannaCry, reportedly impacted systems of public and private organisations worldwide. Within a day, WannaCry had spread around the world, infecting more than 230,000 computer systems in 150 countries and costing approximately $4 billion in financial losses. At the time, it was the largest ransomware attack of its kind.

This global cyber security challenge was only solved through access to global data samples, which allowed a UK-based researcher working for a US company to reverse engineer the malware and discover/deploy a kill switch to immunise the world. If this UK-based researcher was only able to access UK data because other countries had data localisation policies, it could have taken significantly longer to address wannacry and thousands more victims may have been impacted.

5) Impacts to Integrated Enterprise Management Of Cyber Security

Data localisation policies may impact the ability of organisations - particularly those operating in multiple jurisdictions - to adopt an integrated approach to managing cyber security, as illustrated by Swire and Kennedy-Mayo's 2022 paper. Swire and Kennedy-Mayo looked at ISO 27002 cyber security risk management controls and found that 13 of the14 ISO27002 controls, as well as numerated sub-controls, were affected when globalised management of data (particularly security data) shifts to the management of segregated national systems.[18] The impacted controls range from those that address asset management, and security operations - including logging, audit and monitoring, security communications, and information security incident management. Swire and Kennedy-Mayo also note that data localisation may impact an organisation's ability to establish and benefit from an efficient division of labour. For many large multinational companies, their cyber security experts may reside only in a few countries, however, with data localisation those same roles and functions may need to be performed in each country with a localisation regime. This may not only adversely affect the organisation but also domestic small to medium businesses who may not be able to compete with larger companies for finite local talent.[19]

Given the debilitating impact that restrictions on the free flow of security data can have on cyber security, we would urge governments to carefully consider data localisation policies. In developing any data policies, we would encourage the Australian Government to:

- Distinguish between the different types of data across the economy - specifically the difference between content data and security data - and recognise that policies should be nuanced accordingly,
- Ensure that security data can freely flow across jurisdictional borders in real-time to ensure our collective cyber defence, and

[18] P Swire and D Kennedy-Mayo, 'The Effects of Data Localization on Cybersecurity', Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905
[19] Ibid.

- Develop and encourage the widespread adoption of security policies and controls that improve the security of data - beyond the physical location of data. These include implementing strong encryption (at rest and in transit), granular permissions, access management controls and implementing BYOK controls - all of which help securely store and handle data.

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

We appreciate the Government's efforts to harmonise data regulation across all jurisdictions, and would also appreciate a focus on harmonising regulations within the Federal jurisdiction itself.

1) Streamlining Regulation and Policy at Federal Level

As Figure 3 in the discussion paper — "Existing Australian Government data bodies" highlights, companies are dealing with an increasingly complex regulatory landscape, with multiple federal agencies imposing the same and/or similar obligations.

To highlight this point, we draw on one example with respect to reporting obligations:

● 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 data irrespective as to 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 ACSC in accordance with the Security of Critical Infrastructure Act 2018 (in addition to the OAIC).

● The Security of Critical Infrastructure Act 2018 requires regulated companies to report cyber incidents to the ACSC even if the incident is not related to personal information/data. However, should the cyber incident impact personal information/data, they would need to report both the ACSC and the OAIC.

Both the ACSC and OAIC have two different mechanisms to report breaches and reporting timeframes under the two Acts are different.

While we recognise that the two regimes were established with different intentions, with the rise of ransomware attacks compromising personal data, these two regimes are increasingly overlapping - duplicating reporting obligations and creating a regulatory burden. We note the discussion paper's comment that "it is important to recognise that these legislative and policy initiatives were developed and introduced for specific purposes, and typically revolved around a single type of information or storage concern." However, while these reporting structures were established to align with government

agencies and their functions, they may no longer reflect the experience of the public, Industry or the realities of the modern day cyber threat landscape. We would recommend that the Government review these reporting requirements and consider a single reporting agency and mechanism for all data/cyber breaches - irrespective of the circumstances by which the breach occurred or the nature of the information that has been compromised. This will relieve the regulatory burden placed on industry and ensure the public and private sector work efficiently to protect our digital assets.

We also note that successful cyber incident/data breach reporting frameworks will focus narrowly on incidents of a certain threshold/criticality; that reporting timelines are sufficient for victim entities to understand an incident's scope and scale, and deploy mitigations across impacted systems; and that reporting requirements focus only on incidents that have actually occurred (as opposed to "imminent" incidents). Blanket or broad reporting obligations can unintentionally harm the affected organisation and the Government - as organisations are busy reporting to (sometimes multiple) government agencies instead of addressing time-sensitive cyber threats thus allowing cyber attackers to have an advantage. In the rush to meet the reporting timeframe, affected organisations may also report inaccurate or inadequately contextualised information that might be shared further with the Government and potentially other impacted entities, but that will not be helpful.

Finally, and more broadly, we would encourage the DHA to coordinate and align its Plan with work already underway across the Government - in particular the Attorney-General's Department's review of the Privacy Act.

2) *Common Security Standards Across Federal, State and Territory Governments*

As the report notes there is "no national standard for assessing and marking the sensitivity of government data holdings — each jurisdiction has its own security classification system — and in turn, no common standard for the protection of similar data sets held by different jurisdictions." We would support the adoption of a common existing standard to secure government data across the Federal, State, and Territory levels. While at the Federal level, government agencies leverage both the Infosec Register Assessors Program (IRAP) and the Hosting Certification Framework (HCF) to assess whether an organisation/technology product sufficiently manages the security risks to their data, these programs are not widely or formally leveraged by State and Territory Governments. Australian Governments may want to consider leveraging a common standard (such as IRAP) to support their security posture.

Conclusion and about Palo Alto Networks

We would be happy to discuss our ideas further. For more information, please contact Sarah Sloan, head of government affairs and public policy, Australia and New Zealand, at sasloan@paloaltonetworks.com.

About Palo Alto Networks

Palo Alto Networks is the world's cyber security leader. We innovate to outpace cyberthreats, so organisations 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 cyberattacks. Palo Alto Networks undertakes a range of activities that contribute to strengthening Australia's cyber security posture, including actively supporting governments at the operational and strategic levels. We continue to share our cyber security expertise with governments via policy submissions, 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 cyber security professionals. We provide Australian academic institutions with curriculum, technology, and faculty training at no cost via our Cybersecurity Academy Program. To date, we have 28 Authorised Cybersecurity Academy Centres in Australia. 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/