28 August 2025

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

Re: Submission on Horizon 2 Paper

Thank you for the opportunity to provide our perspective on the Horizon 2 paper and the broader outlook for Australian cybersecurity. As a leading global cybersecurity company, Palo Alto Networks is committed to a secure future for all Australians. Our comments and recommendations are informed by our deep understanding of the evolving threat landscape and our experience at the front lines of cyber defence.

Of particular importance is the rise of AI and how it is introducing new risks that can impact Australia's national and economic security, amongst others. Our submission highlights the critical need to secure this new frontier and the emerging AI economy. Key AI security recommendations are:

1. **Securing the AI Lifecycle**: We believe that securing AI systems must be a "first principle" of any AI governance process. The government should adopt a unified security approach that spans the entire AI lifecycle, from its development to its deployment. This *Secure AI by Design* approach involves requiring companies to discover, assess, and protect AI models to continuously evaluate and manage security risks.
2. **AI for Cyber Defence**: While adversaries will use AI to create more sophisticated attacks, we must also harness its power for defence. We recommend policies that incentivise the adoption of AI/ML-driven cybersecurity solutions to enable defenders to neutralise threats with unprecedented speed.
3. **International Alignment on AI Security**: To effectively secure AI, we suggest that Australia engages in international forums to shape rules and standards, advocating for a "secure by design" approach and alignment with global frameworks, such as the NIST AI Security Risk Management Framework.

Here are our responses to your questions 1,2,3,4,12,13 and then 18 to 50:

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should the Government be exploring for cyber security under Horizon 2?

The next few years will be defined by an escalating cyber threat landscape, where the speed, scale and sophistication of attacks will be powered by artificial intelligence. To meet this challenge, we believe the Australian government should be exploring the following key trends and strategic factors for Horizon 2:

- **AI-powered Defence:** The exponential growth of AI presents a dual-use challenge. While adversaries will leverage AI to create more sophisticated attacks, we must harness its power to build a more resilient defence. We recommend advancing policies that incentivise the adoption of AI/ML-driven cybersecurity solutions, to enable defenders to anticipate, track, and neutralise threats with unprecedented speed.
- **The Zero Trust Framework:** The traditional perimeter-based security model is no longer effective. We recommend that the government continue to promote Zero Trust principles as a baseline for all organisations. This involves a "never trust, always verify" approach, ensuring that every user, device, and application is continuously authenticated and authorised before granting access.
- **Facilitating the Free Flow of Security Data:** Cyber adversaries operate without borders. To effectively counter them, security data must be able to flow freely, both domestically and internationally, in real-time. This is critical for training AI/ML models to identify and respond to global threats and for enabling a collective defense.
- **Incentivising the Private Sector:** Rather than relying solely on complex and often slow regulations, we believe the government should focus on incentives to drive cybersecurity uplift. This includes leveraging government procurement as a transformative tool to influence supply chain security and encouraging the adoption of best practices through positive reinforcement.
- **Securing the future AI economy:** Securing the future AI economy is strategically important. Governments must recognize that AI systems introduce new threat vectors and attack surfaces not addressed by existing cybersecurity tools. We recommend a unified, "security by design" approach spanning the full AI lifecycle, from development to deployment, to protect citizens, ensure compliance, and foster innovation.
- **Simplification and lowering total cost of ownership:** Fragmented cyber security tools increase strategic risk for governments and businesses when modernizing their digital infrastructure. Organizations use an average of 83 tools from 29 vendors, hindering visibility and delaying response. Simplifying into a unified security platform enhances operations, accelerates threat detection, and delivers up to 4x ROI. This enables secure digital transformation and enhanced trust, aligning security with policy goals.

2. Collaborating across all levels of Australian Government - Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

While we do not have specific recommendations on current State or Territory initiatives, we would like to see the government expand and replicate programs that:

- **Harmonise Cybersecurity Regulations:** We believe that the current multi-jurisdictional regulatory landscape can create unnecessary complexity and burden for businesses. We support efforts to streamline and harmonise cybersecurity laws across all levels of government to create a more cohesive and efficient compliance framework.Specifically, flow down of cybersecurity regulations and standards from Federal to state, territory and local government levels should be harmonised to reduce complexity and risks. For example, Essential 8 and ISM compliance is dictated for Federal Entities including the specific requirement to leverage IRAP assessed PaaS/SaaS services. However, these requirements do not flow down to all states and local governments, specifically the requirement to utilize IRAP assessed PaaS/SaaS. As a result, the level of cyber security can vary significantly and in some cases result in adoption of PaaS/SaaS solutions that are a risk to security and data sovereignty.
- **Integrate Private Sector Expertise:** To ensure policy and strategy are grounded in real-world threat intelligence, we recommend that the government include private sector experts from cybersecurity and incident response companies as standing members on key advisory boards and committees. This would provide continuous, real-time insights from the front lines of cyber defence.

3. Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes - Does the high-level Model resonate and do you have any suggestions for its refinement?

We believe any high-level model for evaluating cybersecurity outcomes must be flexible, risk-based, and focused on quantifiable results. The model should resonate with the private sector by:

- **Embracing a risk-based approach:** The model should be adaptable to the unique risks and circumstances of different organisations, allowing them to prioritise actions based on their specific needs.
- **Prioritising Measurable Metrics:** We suggest refining any model to focus on metrics that provide clear, quantifiable data points, such as mean time to detect (MTTD) and mean time to respond (MTTR). These metrics provide a tangible way to measure the effectiveness of cybersecurity investments and compliance programs.
- **Recognising Proactive Defense:** The model should place a strong emphasis on proactive defense measures, such as threat blocking at scale and the implementation of Zero Trust principles, to measure not just how an organisation reacts to an attack, but how it prevents one in the first place.

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

Collecting the right data is paramount to effectively monitoring outcomes. We suggest the following methods:

- **Risk-Based Ransomware Reporting**: To gain a clearer picture of the threat landscape, we would encourage the government to support risk-based ransomware reporting that focuses on tactical intelligence and giving other critical network operators mitigations and techniques to better protect their systems.
- **Real-time Threat Intelligence Sharing:** By facilitating the free and real-time flow of security data, we can leverage AI and machine learning to analyse vast datasets and identify emerging threats and new adversarial tactics.
- **Incident Response Data:** Our incident response teams collect valuable data and feedback from cases that can be used to inform policy and refine the outcomes model. This real-world intelligence provides insights into the latest techniques used by adversaries.
- **Independent Evaluations and Benchmarks:** The government should leverage and promote independent, third-party evaluations, such as the MITRE ATT&CK evaluations. These provide an objective and rigorous way to measure the effectiveness of cybersecurity solutions and collect data on how they perform against real-world threats.
- **Attack Surface Management (ASM):** Integrate ASM to establish a baseline of Australia's national cyber posture. ASM provides near real-time discovery and visibility of all network attack surfaces, internal and external, aiding in identifying potential attack vectors and risks. Continuous monitoring of these surfaces, particularly in critical sectors, will be invaluable for assessing the (direction of the) nation's overall cyber posture and the effectiveness of government policies and incentives.

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is the threat evolving or changing?

Palo Alto Networks has a deep understanding of the ransomware threat as our insights are informed by our Unit 42 threat intelligence and incident response team, which handles thousands of cases globally, including in Australia. We've seen firsthand how these attacks exploit the limited resources and expertise often found in smaller organisations.

We recognize that SMBs and individuals are prime targets because they often lack dedicated IT security teams, have limited budgets for security, and may not have a mature security posture. This makes them more susceptible to common attack vectors like phishing emails and exploiting unpatched software vulnerabilities.

The Evolving Nature of Ransomware: The ransomware landscape is constantly evolving, with a clear trend toward more aggressive and sophisticated tactics.

- **Multi-Extortion Tactics**: Ransomware attacks have moved beyond simply encrypting data. Threat actors now commonly use "double extortion," where they first exfiltrate sensitive data before encrypting a victim's network. The ransom demand then includes a threat to publicly leak or sell the stolen data if payment is not made. This tactic significantly increases pressure on victims and can lead to severe reputational damage and regulatory penalties. We've even seen "triple extortion" where attackers also use DDoS attacks or harass customers and employees to force a payment.
- **Ransomware-as-a-Service (RaaS)**: The professionalisation of cybercrime has been a major driver. RaaS platforms provide easy-to-use tools and services, lowering the barrier to entry for less-skilled criminals. This business model has made ransomware attacks more accessible and widespread.
- **Shift in Attack Vectors**: While phishing and exploiting public-facing applications remain common, we're seeing an increase in the use of legitimate, dual-purpose tools for malicious activities. Attackers use tools like WinRAR to compress and exfiltrate data, and backup utilities to push stolen data to cloud storage. They also leverage AI to create more convincing phishing emails and social engineering campaigns.
- **Targeting of Vulnerable Sectors**: While manufacturing and professional services are frequent targets, we've observed a concerning rise in attacks against vulnerable sectors like schools and healthcare, which can have devastating societal impacts.

13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?

The Australian Government can further support businesses and individuals by leveraging the principles of prevention and modern security frameworks.

- **Promote a Zero Trust Architecture**: Palo Alto Networks advocates for the widespread adoption of a Zero Trust security model. A Zero Trust approach, unlike traditional perimeter-based security, operates on the principle of "never trust, always verify." It assumes that threats can exist both inside and outside the network, and therefore requires continuous authentication, validation and authorisation for every user, device, and application. This is a powerful defence against ransomware because it limits an attacker's ability to move laterally across a network and infect multiple systems, significantly reducing the "blast radius" of any breach. The government could promote this model through educational initiatives and provide guidance on implementing its principles, as will be outlined in the future release of the Department of Home Affairs Guiding Principles to embed a zero trust culture.
- **Incentivise Proactive, Prevention-Based Security:** Many smaller entities struggle to implement security due to cost and complexity. The government can encourage a shift from reactive security (detection and response after an attack) to a proactive, prevention-based approach. The government could look to create recommended blueprints (similar to CISA has done for reference Zero Trust Architectures) that could reduce the complexity and effort for smaller entities to uplift and adopt a Zero Trust Culture. These recommended architectures and implementation guidance could be further enhanced by the government providing a rebate scheme for the procurement and

implementation of Zero Trust architectures for small to medium businesses which would in turn benefit the Australian community by reducing the cost of cybercrime by preventing or limiting ransomware attacks.

18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

We believe Australia should look to international best practices that prioritise a Zero Trust, platform-based approach to security, rather than a fragmented, siloed one. The most effective models are those that are outcomes-focused and adaptable to the unique needs of different technologies. A number of NIST Special Publications, in particular, provide useful frameworks for secure technology best practices, related to Zero Trust Architecture, 5G Cybersecurity, and AI Security Risk Management Framework.

- **Zero Trust for Operational Technology (OT) and Critical Infrastructure:** The convergence of IT and OT environments requires a new security paradigm. We see the most effective international examples moving away from a perimeter-based "air-gapped" security model for OT. Instead, they are adopting a Zero Trust approach that applies least-privilege access controls, microsegmentation, and continuous verification. This is particularly crucial for critical infrastructure and edge devices, where a single compromise could have catastrophic physical consequences.
- **Edge Devices and IoT Security by Design:** For the proliferation of Internet of Things (IoT) and edge devices, best practice is to mandate a "security by design" standard. Instead of retrofitting security, Australia should consider frameworks that require security to be built into products from their inception. This includes continuous device profiling, vulnerability management, and automated policy enforcement, which can be achieved through a unified platform that secures both IT and OT environments. We believe a platform-based approach is critical for managing the vast and diverse number of edge devices.
- **Adoption of converged IT/OT framework:** Many OT systems are leveraging physical air gaps as a primary pillar for achieving security in OT environments. Air gap methodologies in a contemporary technology landscape can lead to the adoption of legacy technologies with limited efficacy whilst resulting in increased complexity and decreased security visibility. Providing regulatory settings and incentives for organisations to adopt converged IT/OT environments will help to provide increased security visibility and uplift for OT environments whilst reducing complexity for the adoption of Zero Trust.
- **Critical and Emerging Technology (CER) Frameworks:** For CER, such as AI, 5G, and quantum computing, international best practices involve a focus on risk management and transparency. Australia should consider frameworks that guide the assessment of risk throughout the technology lifecycle, from development to deployment. The government's role should be to set clear, performance-based standards and empower the private sector to innovate within those boundaries.

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

We believe that empowering consumers requires a multi-faceted, collaborative approach between government and the private sector.

- **Public-Private Education Campaigns:** The government could partner with cybersecurity leaders like Palo Alto Networks to develop and deliver national public awareness campaigns. These campaigns would not just focus on generic advice but provide actionable, real-world guidance on how to secure devices and recognize threats.
- **Secure Product Labeling:** We support an initiative where technology products are voluntarily and transparently labeled with a clear security rating. The government should work with industry to develop a simple, recognisable labeling system that consumers can use to make informed purchasing decisions. This approach would incentivise manufacturers to build more secure products while also educating consumers on the importance of product security.
- **Free and Accessible Resources:** Palo Alto Networks is already committed to providing educational resources through our Cybersecurity Academy and certification programs. We believe this model can be scaled through government partnerships to offer free, foundational cybersecurity training to end-users and small businesses, equipping them with the skills to protect themselves from common threats.

20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

As a global company operating in over 150 countries, we understand that trust and transparency are paramount. We believe the government can provide valuable guidance by:

- **Developing a Transparent, Risk-based Framework:** We need clear, consistent, and predictable guidance on how to assess and manage foreign ownership, control, or influence risks. This framework should be transparent and based on a thorough risk assessment, avoiding broad, protectionist policies that may limit access to global innovation.
- **Promoting a Platform-centric Approach:** The government should provide guidance that encourages a platform-based security model. A unified security platform, such as ours, reduces complexity and offers consolidated visibility and control, making it easier to manage supply chain risks and ensure that security policies are consistently enforced across the entire technology stack.
- **Strengthening Procurement Policies:** The government's procurement process is a powerful tool. By providing clear guidance on the security standards required for technology vendors, it can incentivise a higher level of security across the entire ecosystem, regardless of a company's country of origin.

21. How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

Data is the lifeblood of the modern economy, and its secure transfer is non-negotiable. To better understand and secure it, the government should:

- **Foster Information Sharing:** The government and industry must create a framework that enables real-time, bidirectional data sharing on cyber threats. By working with companies like ours, which have a global view of the threat landscape, the government can gain invaluable insights into how malicious actors are attempting to exploit data.
- **Facilitating the Free Flow of Security Data:** Cyber adversaries operate without borders. To effectively counter them, security data must be able to flow freely, both domestically and internationally, in real-time. This is critical for training AI/ML models to identify and respond to global threats and for enabling a collective defense.
- **Leverage AI for Visibility:** We offer technologies that provide deep, real-time visibility into application and data flows. The government should partner with us to develop policies that encourage organisations to use AI-driven tools to classify and monitor data in transit, which is critical for identifying unauthorised data access and exploitation.
- **Establish a "Data in Motion" Policy:** We recommend a policy framework that specifically addresses the security of "data in motion" and encourages the use of advanced security controls, such as our Content-ID and enterprise DLP technologies, to prevent data exfiltration and block malicious transfers.

22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

We believe that innovation and security are inextricably linked. To achieve this aim, government and industry must collaborate on:

- **Establish Secure AI by Design Principles:** In an AI-forward world, we must foster safe innovation by empowering organisations to harness the benefits of AI while securing AI-powered application and model development and use. As part of this framework, the government should look at frameworks that encourage organisations to *Discover* models operating on their networks, to gain a clear understanding of AI assets being developed across the enterprise; *Assess* AI models to continuously evaluate security, safety, and compliance risks of AI apps, agents, models and datasets, across the supply chain and runtime; and *Protect* AI systems to detect and prevent risks detected both in the supply chain and in the model's runtime.
- **Zero Trust and IP Protection:** IP theft is a significant threat to Australia's economic prosperity. A Zero Trust model is the most effective defense, as it assumes no user or device can be trusted by default. Government and industry should work together to

implement this principle, ensuring that access to sensitive IP is continuously verified and protected.

- **Enhancing Forensic Capabilities:** The government can work with industry experts, such as our Unit 42 threat intelligence team, to develop and share best practices for digital forensics. This will help organisations not only prevent IP theft but also respond effectively when a breach occurs, ensuring that valuable evidence is preserved for legal recourse.
- **Promoting a Secure Global Supply Chain:** The government and industry must work together to ensure the security of the entire supply chain. By setting and enforcing secure standards for all vendors and partners, Australia can create a trusted environment where data can be shared with confidence, boosting innovation without compromising security.

23. What guidance can the government provide to support the safe and responsible uptake of critical and emerging technologies?

The government has a vital role to play in guiding the responsible adoption of new technologies. We recommend the following guidance:

- **Risk-based and Technology-agnostic Principles:** The government should provide guidance based on risk management principles that are technology-agnostic. This will ensure that the guidance remains relevant as technologies evolve. For example, instead of creating rules for a specific AI model, the guidance should focus on managing the risks associated with AI's use of data, its potential for producing biased responses or hallucinations , and its security vulnerabilities.
- **Clear Security Baselines:** The government should establish and promote clear security baselines and best practices for critical and emerging technologies, such as our Zero Trust for OT framework. This provides a clear roadmap for organisations to follow while still allowing them the flexibility to innovate.
- **Public-Private Sector Collaboration Forums:** The government should create formal, ongoing forums where industry leaders can collaborate with policymakers to discuss the security implications of emerging technologies. This will ensure that guidance is informed by real-world expertise and is practical for industry to implement.

24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

The government can best support industry by creating a framework that incentivises a shift from reactive to proactive security. Australia's proactive cyber posture for industry should look like this:

- **A "Prevention First" Mindset:** Instead of focusing on detection and response after an attack has occurred, our national posture should prioritise blocking threats before they

can even reach their targets. This means leveraging automated, inline security controls that use real-time threat intelligence to prevent known and unknown attacks.

- **Zero Trust as a Foundation:** The proactive posture must be built on Zero Trust principles. This means that instead of trusting and then verifying, organisations must continuously verify every user, device, and application and apply least-privilege access, even within their own networks.
- **A Platform-Based Approach:** The government should encourage industry to move away from a fragmented collection of point security products. A consolidated security platform provides a unified view and control across the entire attack surface—network, cloud, and endpoint—enabling more effective and automated threat prevention.
- **Facilitate the sharing of threats, Not Just Incidents:** To truly be proactive, the government should work with industry to encourage the reporting of malicious activity and threat intelligence, not just post-mortem reports on successful breaches.

25. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

Yes, we believe it is essential for the government to clearly scope and define what a proactive cybersecurity posture should look like for industry. This provides the necessary clarity and a common goal. The government's role is not to dictate specific products but to articulate the outcomes required for a proactive posture. This definition should be based on a clear set of principles, such as those mentioned above (Prevention First, Zero Trust), and backed by a transparent, risk-based framework. A defined posture provides a measurable benchmark for organisations to aim for, which is crucial for building a more resilient national ecosystem.

26. How could government further support industry to block threats at scale?

The most impactful way the government can support industry in blocking threats at scale is through a "Clean Pipes" initiative. We have previously advocated for this approach, where Internet Service Providers (ISPs) are encouraged or required to provide a default level of security for their customers. This means:

- **Government-Industry Collaboration:** The government should partner with ISPs and leading cybersecurity companies to create a centralised, shared threat intelligence feed.
- **Encourage Threat Blocking:** A policy that encourages ISPs to automatically block known malicious domains, phishing sites, and malware command-and-control servers at the network level. This provides an immediate and effective layer of defense for all customers, especially those with limited resources, such as small businesses and consumers.

27. How could the use of safe Browse and deceptive warning pages be amplified?

The amplification of safe Browse and warning pages is a key component of a proactive defence. We believe this can be achieved through:

- **Standardised Browser-level Integration:** The government could work with major browser developers to create a national standard for safe Browse. This would ensure that deceptive or malicious content is flagged consistently, regardless of the browser or device.
- **Policy-driven Warnings:** Our advanced URL filtering and threat prevention technologies can enforce "safe search" policies and block access to harmful sites at the network level. The government could incentivise organisations to adopt these technologies and use our customisable warning pages to educate end-users on why certain sites are blocked, thereby turning a security control into a teaching moment.
- **Real-time Intelligence Feeds:** To ensure these warnings are as accurate as possible, the government should facilitate the real-time sharing of threat intelligence on malicious domains and URLs with technology providers.

28. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

To support a thriving threat-sharing ecosystem, we need to move beyond simple information exchange to an "intelligence-enabled" framework.

- **Real-time, Automated Sharing:** We need a system that allows for the automated, real-time sharing of actionable threat intelligence, such as Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs). Our Unit 42 threat intelligence team already participates in international threat-sharing partnerships, and this model could be replicated and scaled domestically.
- **New ISACs:** We believe that any sector that is critical to the Australian economy or community, particularly those with low cybersecurity maturity, should have a dedicated Information Sharing and Analysis Center (ISAC). This includes the agriculture, transportation and logistics, and education sectors. One specific initiative to consider is to include sector identifiers tagged to IoCs within the Cyber Threat Intelligence Sharing (CTIS) program that could enable automated release of threat intelligence to flow down from Australian Signals Directorate to the relevant sector ISAC within releasibility frameworks.
- **Remove Holding Factors:** The primary factors holding back the creation of these ISACs are often a lack of funding, a fear of liability from sharing sensitive information, and a lack of trust between competitors. The government can address this by providing funding, offering legal protections for good-faith sharing, and helping to build a culture of collaboration.

29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

Aligning intelligence sharing for both cybersecurity and scams requires a unified approach.

- **Unified Intelligence Platform:** We must move away from siloed intelligence on cyber threats and scams. The government should work with industry to create a unified platform where threat intelligence from our global network and scam-related data from consumer reports can be combined.
- **AI-powered Analysis:** This combined intelligence should be analysed with AI and machine learning to identify both existing and future attack patterns, actor profiles, and shared infrastructure between cyber-attacks and scam campaigns.
- **Operationalising Intelligence:** The shared intelligence should be immediately operationalised into threat-blocking controls. For example, a fraudulent website identified by a scam report should be automatically added to threat intelligence feeds and blocked at the network level.

30. Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

The roles and responsibilities in a cyber conflict or crisis are still not entirely clear and require ongoing clarification. The government's role is to provide strategic leadership, national-level threat intelligence, and a legal framework for a coordinated response. Industry's role is to defend its own networks and critical infrastructure, and to provide technical expertise and threat data to the government. To improve preparedness, we believe the government should:

- **Conduct Advanced, Full-Scale Cyber Exercises:** The government's regular joint cyber exercises with critical infrastructure providers and leading cybersecurity companies is important and should be continued. These exercises need to move beyond tabletop scenarios and simulate a full-scale, multi-vector attack, testing response plans, communication channels, and the resilience of critical systems.
- **Membership of standing Cyber Incident Response Board (CIRB):** This board needs to include representatives from the government and key private sector partners. It would provide a formal, pre-established channel for communication and coordination during a crisis, ensuring that the best minds from both sectors can collaborate in real time.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

We believe the government can better incentivise businesses by:

- **Creating a "Safe Harbor" Framework:** Many organisations are hesitant to adopt vulnerability disclosure policies for fear of legal liability. The government could create a safe harbor framework that protects businesses from legal action, as long as they are acting in good faith and following their disclosure policy.
- **Leveraging Procurement:** The government should use its procurement power to set a clear standard. By making vulnerability disclosure policies a required component for all vendors, it would create a powerful market incentive for businesses to adopt them.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Yes, absolutely. We believe that Australia should have a formal vulnerability disclosure program. This is a critical component of a proactive national security posture. A national program would:

- **Provide a Clear Mechanism:** A formal program would provide a clear and safe mechanism for security researchers to report vulnerabilities without fear of legal reprisal. This is vital for maintaining a strong relationship with the security community, which acts as a valuable, and often free, resource for finding and fixing weaknesses.
- **Centralise and Triage Reports:** A national program could act as a central hub for vulnerability reports, triaging them and ensuring they are directed to the appropriate organisations.
- **Promote Responsible Disclosure:** By providing a structured program, the government can help enforce responsible disclosure, ensuring that vulnerabilities are fixed before they are made public, thereby protecting Australians from harm. Palo Alto Networks has its own responsible disclosure policy, and we believe a national program would align with these best practices and benefit the entire ecosystem.

Palo Alto Networks appreciates the opportunity to provide our perspective on the "Shield 4: Protected critical infrastructure" framework. We believe that securing Australia's critical infrastructure is paramount for our national security, economic prosperity, and way of life. Our views are informed by our global experience in securing critical infrastructure sectors, including those with sensitive operational technology (OT) environments.

33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

We support the underlying objectives of the SOCI Act and acknowledge its importance in strengthening Australia's cyber resilience. We have engaged with the government on the development of this legislation and believe its core intent is sound.

However, we have voiced concerns about certain aspects of the Act. We believe the legislation, in its current form, requires greater clarity to be truly well-understood by the industry. The obligations must strike a careful balance: they need to be prescriptive enough to drive a tangible uplift in security, but also flexible enough to be implemented by a diverse range of critical infrastructure entities, from large corporations to smaller operators.

- **Proportionality and Enforceability:** While the intent is to be proportionate, some of the powers within the Act could benefit from stronger checks and balances. We have previously recommended legislated appeal and review rights for certain provisions to ensure the powers are exercised fairly and transparently. We are also concerned that a one-size-fits-all approach to regulatory burden may not be proportionate to the risk faced by all entities.

34. Are there significant cyber security risks that are not adequately addressed under the current framework?

Yes, we believe there are several key risks that require more explicit attention within the current framework:

- **The IT-OT Convergence:** The SOCI Act's focus often leans heavily on IT-centric threats, but the growing convergence of IT and OT networks in critical infrastructure is creating new and significant risks. The unique nature of OT—where availability and safety are prioritised over confidentiality—requires a different approach. The current framework could be more explicit in addressing the specific cybersecurity challenges of OT environments, including vulnerabilities in legacy systems and the need for a Zero Trust approach to microsegmentation.
- **Supply Chain Security:** While the Act touches on supply chain risks, a more robust and granular framework is needed. The dependency of critical infrastructure on global and complex supply chains means a single vulnerability in a third-party vendor could have a cascading effect. The framework should provide clear guidance and incentives for entities to assess and mitigate risks from their entire supply chain.
- **Lack of a Unified, Proactive Posture:** The current framework, with its focus on incident reporting, can be perceived as reactive. It does not sufficiently mandate a proactive, prevention-first security posture. This leaves a significant gap, as an organisation should be focused on preventing an attack from occurring in the first place, rather than simply being able to respond to it.

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

We believe the regulatory burden, particularly for smaller entities, may not be fully proportionate to the risk and outcomes being sought. The risk management programs and reporting obligations can be complex and costly for organisations that lack the resources of larger corporations. Our recommendation is to:

- **Streamline Regulations:** The government should work to streamline and harmonise regulations across sectors and between different pieces of legislation to reduce duplicative efforts and lower the compliance burden.
- **Incentivise, Don’t Just Regulate:** We continue to believe that incentivising good security practices is often more effective and efficient than solely relying on regulation. Incentives, such as tax credits for cybersecurity investments or preferential treatment in government procurement, can empower a broader range of entities to uplift their security posture.

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

The government has a crucial role to play in enabling uplift. We believe the following support would be most effective:

- **Clear, Technology-Agnostic Guidance:** Government should provide practical, technology-agnostic guidance and reference architectures, based on international best practices like Zero Trust and AI-driven automation. This provides a clear roadmap without mandating specific products.
- **Incentives for Adoption of Best Practices:** The government could offer incentives for adopting advanced security technologies.
- **Cybersecurity Education and Workforce Development:** A shortage of skilled professionals is a key challenge. The government should expand programs like our Cybersecurity Academy, which provides free curriculum and training to academic institutions, to build a national workforce capable of managing sophisticated OT and IT security.

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

The government can support private sector partners by making its security requirements more accessible, transparent, and collaborative.

- **Harmonise Requirements:** The government should strive to harmonise its various security requirements and certifications (e.g., PSPF, IRAP) and make them easier to navigate. This would reduce the compliance burden for organisations that work with multiple government agencies.
- **Co-design and Collaboration:** The government should engage the private sector in the co-design of its security requirements. This ensures that the controls and certifications are technically feasible, reflect real-world threats, and align with global industry standards. We have participated in such discussions and believe a formal, ongoing forum would be highly beneficial.
- **Clear Procurement Policies:** The government's procurement rules are a powerful tool for driving security uplift. By setting clear security requirements in procurement and providing clear guidance on how vendors can meet them, the government can encourage the private sector to prioritise security in its offerings.

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

Based on our engagement with the Australian private sector, government security requirements and frameworks are increasingly being considered and adopted, particularly in critical infrastructure. However, the adoption is not uniform.

- **Leading Companies are Adopting:** Many large critical infrastructure operators and security-mature organisations are proactively aligning with or seeking certifications for frameworks like the IRAP and the Information Security Manual (ISM). They see this not

only as a compliance requirement but also as a way to demonstrate a high standard of security to their partners and customers.

- **Challenges for Broader Adoption:** For many other organisations, especially smaller ones, the adoption of these frameworks can be a significant challenge due to a lack of resources, technical expertise, or a clear understanding of the requirements.
- **A Common Language:** We are seeing that government frameworks are providing a "common language" for security. For example, Zero Trust principles, which are central to many government security discussions, are increasingly being adopted by the private sector as the preferred security architecture. We are a key enabler of this transition, with solutions that allow both government and private entities to implement Zero Trust across their networks, clouds, and endpoints.

Palo Alto Networks is pleased to continue this discussion on "Shield 5: Sovereign capabilities." We believe that a strong sovereign capability is not about isolation but about smart, strategic investment in people, partnerships, and resilient technology. Our commitment is to help Australia build a world-class cyber workforce and ecosystem that is prepared for the challenges of today and tomorrow.

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

The government has a vital role to play as a facilitator, unifier, and strategic partner in developing Australia's cyber workforce. We believe the following initiatives would best support industry growth:

- **Expanding Education with the Cybersecurity Academy:** We have demonstrated a successful model with our Cybersecurity Academy, which provides free, turnkey curriculum and resources to academic institutions. The government can support this model by incentivising more academic institutions to adopt these programs and by partnering with companies like ours to scale them across the country. This ensures students, from high school to university, are learning on the technology that is used in the real world.

  National Certification and Skills Framework: The government should work with industry to develop a national certification framework that is aligned with globally recognised standards. This would provide a clear career pathway, ensuring that training and certifications are relevant to the needs of the job market.

- **Incentivising Apprenticeships and Internships:** Policies that provide financial incentives, such as tax credits or grants, for companies to offer internships and apprenticeships would be highly effective. This gives new talent the essential on-the-job experience required to enter the workforce.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

Our experience and research suggest that successful initiatives for mid-career transitions and diversity are those that focus on skill-based training and mentorship.

- **Targeted Training Programs:** Programs that provide intensive, hands-on training to individuals from different professional backgrounds are most effective. These are often project-based and focus on practical skills rather than just theoretical knowledge.
- **Inclusive Hiring and Mentorship:** Initiatives that promote diversity, equity, and inclusion are crucial. Our own internal programs, for example, focus on empowering diverse talent and creating an inclusive culture where everyone feels valued. We have found that having diverse hiring panels and mentorship programs are key to not only attracting but also retaining talent from all backgrounds.
- **Government-sponsored Traineeships:** The government could pilot traineeship programs that specifically target individuals from non-traditional backgrounds, such as veterans, women returning to the workforce, or those from different industries. These programs could combine government funding with industry-led curriculum and on-the-job training.

41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

We believe that a wide range of industries possess highly transferable skills that could be leveraged to grow the cyber workforce. These include:

- **Creative and Analytical Roles:** Professionals from industries like finance, insurance, law, and data analytics possess critical thinking, problem-solving, and attention to detail skills that are highly valued in cybersecurity roles such as threat intelligence analysis and forensic investigation.
- **Technical and Operational Roles:** We have seen success in transitioning individuals from IT support, network administration, and systems engineering roles into more specialised cybersecurity functions like incident response and security operations.
- **Research and Data:** Our own research and data on threat actors, such as those from Unit 42, show that adversaries often combine technical skills with social engineering and business acumen. This suggests that a diversity of skills is needed for effective cyber defense. Research on skill-based hiring, rather than degree-based, can provide a strong foundation for these efforts.

42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

Effective collaboration requires a structured, ongoing, and results-oriented approach.

- **National Cyber R&D Framework:** The government should lead the development of a national cybersecurity research and development framework. This framework would outline key research priorities and create a clear mechanism for collaboration.
- **Joint Public-Private Research Hubs:** The government should fund and establish joint research hubs that bring together experts from industry, academia, and government. These hubs would focus on solving specific, complex challenges, such as securing critical infrastructure or leveraging AI for defense. Our partnership with institutions on cyber range exercises is a good example of this model.
- **Streamlined Funding and IP Policies:** The government should ensure that funding models for research are agile and that intellectual property (IP) policies are clear and fair. This will encourage the private sector, which invests heavily in R&D, to participate more readily.

43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

We believe the following would enhance partnerships and collaboration:

- **Embedded Specialists:** The government could embed industry and academic specialists within its policy and operational teams, and vice versa. This would build trust, promote a deeper understanding of real-world challenges, and ensure that policy is informed by practical expertise.
- **Joint Policy Development Working Groups:** Create formal working groups for policy development that include a diverse range of stakeholders. This ensures a broad range of perspectives are considered from the outset, rather than simply seeking submissions after a policy is drafted.

44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

In our view, identifying and prioritising sovereign capabilities should be done through a risk-based and strategic lens.

- **Focus on Foundational Skills, not just Products:** Instead of prioritising the development of Australian-made products at all costs, the government should prioritise developing sovereign skills and the ability to operate and secure a wide range of global technologies. A "product-first" approach risks Australia becoming technologically isolated.
- **Identify Critical Gaps:** We should collectively identify and prioritise the most critical gaps in Australia's cybersecurity ecosystem—for example, in OT security, advanced threat hunting, or secure AI. The focus should then be on developing capabilities to fill those specific gaps, whether through local innovation or strategic partnerships.

- **Leverage the Global Ecosystem:** True sovereign capability is not about "going it alone." It's about being able to leverage the best-in-class technology from a trusted global ecosystem, while simultaneously developing the local skills and capabilities to deploy, manage, and innovate on that technology securely.

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

The area of most concern for ICT concentration is a dependency on outdated or insecure technology. True risk does not come from reliance on a trusted and secure global provider but from a fragmented, unmanaged, and vulnerable technology stack. Mitigation strategies should focus on:

- **Platformisation as a Strategy:** The most effective mitigation strategy is to adopt a platform-based approach to security, which consolidates and integrates multiple technologies. This reduces complexity and the number of vendors an organisation needs to manage, while also providing a unified view of the entire attack surface.
- **Vendor Integrity and Supply Chain Security:** The government should focus on a vendor's integrity, security practices, and supply chain security rather than its country of origin. We have previously recommended that the government amend its procurement rules to place a greater emphasis on these factors.
- **Skill Diversification:** The government and industry should invest in building a workforce with diverse skills that can secure a variety of technologies.

Palo Alto Networks is pleased to continue this discussion on "Shield 6: Strong region and global leadership." We believe that Australia's national cybersecurity strategy must extend beyond its borders to be truly effective. Given that cyber adversaries do not respect national boundaries, Australia's leadership in shaping a secure and stable region is essential for its own resilience.

46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

We view attributions, advisories, and sanctions as important but often insufficient tools in isolation.

- **Attributions and Advisories:** Attributions are crucial for holding malicious actors accountable and are most effective when supported by robust, technical evidence. Our Unit 42 threat intelligence team frequently contributes to this global effort, providing threat data and analysis to help identify and expose cybercriminals and state-sponsored attackers. Advisories are a vital tool for providing timely, actionable intelligence to the public and private sectors, enabling them to proactively defend against threats.
- **Sanctions:** Sanctions can be a powerful tool, particularly when applied in a coordinated, international effort. They can disrupt the financial networks and infrastructure of cyber

adversaries. However, to be effective, they must be part of a broader, more comprehensive strategy.

For Horizon 2, we recommend Australia consider developing and using the following tools for cyber diplomacy and deterrence:

- **"All-of-Nation" Cyber Deterrence:** Australia should develop a comprehensive deterrence strategy that goes beyond government actions. This should include a "whole-of-economy" approach that leverages the private sector's capabilities for threat blocking at scale, as well as a strong public-private partnership for coordinated incident response.
- **International Norm-Building:** Australia should actively shape international norms and standards to promote a stable and secure cyberspace. This should include advocating for principles like the free and real-time flow of security data, which is essential for a collective defence against global threats.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

We believe that Australia has a leadership role to play in the region. The Australian government can enhance its engagement by:

- **Cyber Capacity Building:** Australia should continue to invest in cyber capacity-building programs in Southeast Asia and the Pacific. These programs should not only focus on technical skills but also on governance and policy development. We are committed to supporting this effort through our educational programs and by providing access to our threat intelligence and expertise.
- **Shared Threat Intelligence Platforms:** The government could explore the creation of a regional threat intelligence platform, allowing for the real-time sharing of actionable threat data. This would enable a collective, proactive defense against shared threats like ransomware and financially motivated cybercrime. Our own global platform and threat intelligence feeds could be a model for this type of collaboration.
- **Supporting Data Residency and Sovereignty:** We recognise the importance of data residency and sovereignty to countries in the region. Our recent expansion of cloud infrastructure in the Asia-Pacific and Japan region, for example, is designed to help enterprises adhere to local data residency requirements while benefiting from global-scale security. The Australian government could support a similar approach that balances data residency with the need to maintain a global threat picture through the sharing of critical security-related data.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

While we are not directly involved in the Cyber RAPID program, we believe its core mission of providing rapid incident response is critical. We see additional value it could provide by:

- **Strategic Foresight:** Beyond responding to incidents, the program could serve as a platform for strategic foresight. By analysing the data and trends from the incidents it responds to, it could provide a forward-looking view of the regional threat landscape.
- **Building Local Resilience:** The program's greatest value could be in transitioning from a purely responsive role to one that builds lasting, local resilience. This would involve embedding a "train the trainer" component into its work, where it helps local teams develop their own incident response capabilities.
- **Integration with Broader Threat Intelligence:** Cyber RAPID's insights should be integrated into a broader threat intelligence ecosystem, linking its findings with those from governments, industry, and partners like our Unit 42 to create a more comprehensive picture of regional threats.

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

In Horizon 2, Australia should focus its efforts on international forums and issues where it can leverage its expertise and influence to promote a stable and secure cyberspace.

- **Promoting a Proactive Security Model:** Australia should advocate for the adoption of proactive security models, such as Zero Trust and "security by design," in forums like the United Nations, ASEAN, and the Quadrilateral Security Dialogue (Quad).
- **International Standards Bodies:** Australia should play an active role in international standards bodies to ensure that technology standards, particularly for emerging and critical technologies, are industry-led, market-driven, and globally workable. We caution against the development of country-specific standards, which can create fragmentation and ultimately weaken global security.
- **Advocating for a Free Flow of Security Data:** Australia should continue to advocate for the free flow of security data across borders. We have previously submitted that a lack of real-time data sharing can have significant impacts on collective defense, and Australia should work in forums to ensure that data localisation policies do not unintentionally compromise cybersecurity.

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

To effectively align its regulations internationally, Australia should prioritise frameworks that are outcomes-based and promote global security principles.

- **Aligning with Global Frameworks:** Australia should prioritise alignment with globally recognised frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001. This would reduce the regulatory burden on multinational companies and promote interoperability.
- **Zero Trust as a Guiding Principle:** As a foundational principle for security, we believe Australia should align its regulatory requirements with Zero Trust. This principle is

becoming a global standard and would ensure that Australia's regulations are future-proofed against evolving threats.

- **Harmonising with Key Trading Partners:** Australia should prioritise aligning its regulations with key trading partners to create a more seamless and secure digital economy. This could include aligning on issues such as mandatory reporting of ransomware payments and supply chain security standards.

End of Questions and Answers.

About Palo Alto Networks - As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organisations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformisation allows enterprises to streamline security at scale, ensuring protection fuels innovation.

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

In addition to our policy work with Governments, Palo Alto Networks is also committed to growing the next generation of Australian cybersecurity professionals. We provide Australian academic institutions with curriculum, technology, and faculty training at no cost via our Cybersecurity Academy Program. Palo Alto Networks also undertakes activities across our community to raise cyber security awareness and engage the next generation on cyber security issues through our Cyber Safe Kids program. This program educates 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, please contact [redacted]

Explore more at **www.paloaltonetworks.com.**