16 September 2020

Critical Infrastructure Center
Department of Home Affairs
Submitted Online via: https://www.homeaffairs.gov.au

Re: Call for Views - Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

Palo Alto Networks appreciates the opportunity to provide input to the Department of Home Affairs' call for views on the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (the consultation paper).* We congratulate the Australian Government on its leadership on cybersecurity and critical infrastructure (CI) matters to date.

Palo Alto Networks is the largest cybersecurity company in the world. Palo Alto Networks secures the networks and information of more than 75,000 enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cybersecurity posture. We work with some of the world's largest organisations across all industry verticals, including in many CI sectors. We combine our knowledge from working with customers and governments across the world to directly inform our response.

We have addressed some specific questions asked as part of the consultation paper, following some general comments.

General Comments

Palo Alto Networks supports the Government's commitment to taking further action to improve the cybersecurity posture of Australia's CI sectors, as articulated in the *Cyber Security Strategy 2020*. We welcome these efforts and the opportunity to provide input into the proposed new regulatory framework. Before answering some of the questions articulated by the consultation paper, we have the following observations and recommendations.

Recommendation 1: Define "Data and the Cloud"

The meaning of the "Data and the Cloud" sector, which is proposed to be captured under this regulatory framework, is unclear. This makes it difficult for companies to understand to

whom the positive reporting obligations would apply. We understand that the Government may be considering a definition that relates to storage, processing and transmission of data in the context of Australian Governments and where it is "business critical" to CI. It is important that the Government is clear on what business critical could mean in this context - for example, is it data that pertains to research and development, or core to business continuity - and how is the latter defined. By contrast, some of the workshops indicated that the Government is looking to regulate the physical data infrastructure. If this is the case, we recommend the Government consider renaming "data and the cloud" to "data centre providers".

Recommendation 2: Lead by Example - Government Management of Cybersecurity Risks

The Government is asking the CI sector to change how it manages cybersecurity risks - to "mainstream" cybersecurity into their operations and board level conversations. The Government should lead by example in this regard, both in terms of the management of its own cybersecurity and supply chain risks, and in its policy documents. In particular, the Government should update its procurement policies (i.e. the Commonwealth Procurement Rules and the ASDEFCON Suite) to reference both cybersecurity and supply chain security risk. It is important for all Government departments and their officials to consider the security and integrity of the technology, goods and services as part of their procurement processes. This would demonstrate the Government's commitment to cybersecurity and supply chain risk management. The Government should also consider issuing a Departmental directive to include cybersecurity in all key policy documents it produces. Technology permeates every aspect of our lives, and every aspect of Government and its functions - from healthcare, to transport and energy. It is therefore critical that cybersecurity be a key consideration addressed in all Government policies, unless a reasonable exception applies, to ensure that policies, processes and technology are secure by design.

Recommendation 3: Broadly Define "Supply Chain Security" to Encompass Product Integrity

Globally policymakers are increasingly voicing concerns about supply chain security, particularly related to critical infrastructure operations. However, in the Australian context there are varying definitions of "supply chain security" and confusion as to its scope. We would encourage the Australian Government to define supply chain security to include integrity of the ICT products and services that CI sectors procure and use. As part of these regulatory reforms, the Australian Government should require CI to adopt supply chain best practices in line with international standards. This should include transparency in how

operators manage risks to their supply chain mechanisms and how they encourage their ICT vendors, including in the 5G and IoT space, to demonstrate adherence to best practices. Australia should consider the security implications of companies who share the source code of their unique intellectual property (IP) with governments as a condition of access to certain markets. Best practices might include:

- An organisational focus on end-to-end risk management. Supply chain risks should be identified across an entire product lifecycle – design, sourcing, manufacturing, fulfilment, and service – and proactive action should be taken to ensure the integrity of products. Risk assessments should be performed early in the product development lifecycle to help determine the feasibility of product design decisions.
- Strong supplier management focused on security requirements as well as a collaborative relationship to ensure a complete view of suppliers' security posture.
- Geopolitical implications for product integrity, including identifying manufacturing locations that enable companies to more easily manage personnel, facility and product security, and identifying whether suppliers share product source code with other governments.
- Active engagement in public-private partnerships designed to increase collaboration between public and private sector organisations and make recommendations for enhancing supply chain security.
- Finally, executive management buy-in is vital, and strong coordination across business units is critical to successful supply chain risk management.

Government and private industry should work collaboratively to identify other supply chain best practices and develop potential incentives to promote their adoption across all sectors. This work should draw on international best practice.

Recommendation 4: Beyond Guidance and Directives to Prevention - Harden National Defences via Internet Service Providers (ISP) and Telecommunication Security

To stop the economic loss associated with cybercrime and the impacts of a widespread cyberattack, Australia should harden its national defences and address these threats at scale via leveraging ISPs to detect and stop cyberattacks in real time. ISPs and Telecommunication providers (Telcos) should have constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cybersecurity threats within that traffic.[1] We understand that Telstra has adopted a cleaner pipes policy that aims to block the command and control traffic used by cybercriminals once their malware has been installed.

[1] https://www.paloaltonetworks.com/resources/whitepapers/securing-mobile-network-infrastructures

We believe this is a great step in the right direction and suggest the Government determine how it might broaden and scale the Telstra approach, as well as provide incentives (economic or otherwise) for ISPs and telcos to take similar actions to help build Australia's collective defences. It is critical to Australia's national cyber defences that all ISPs maintain constant real-time visibility of traffic passing through their networks and be able to detect and stop real time cybersecurity threats within that traffic.

Recommendation 5: Draw on Existing International Standards

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

Recommendation 6: Draw on International Expertise and Experiences

Australia is not alone in trying to address the challenge of protecting and securing its CI sectors. We recommend that the Australian Government engage with its international partners on best practice in this regard.

Recommendation 7: Release an Exposure Draft of the Legislation

We understand that the Government does not intend to share the exposure draft for the proposed amendments to the *Security Critical Infrastructure Act*. Given the size and scope of

the proposed regulatory framework, we would recommend that the Government share this draft with the affected industries, in addition to any reviews through the Committee processes.

Recommendation 8: Undertake Consultations with Cybersecurity Companies and Involve Cybersecurity Companies in Threat Sharing

We note the Government's call for views on the consultation paper and the associated townhall and workshops mark the beginning of an ongoing consultation with Industry. However, the Government's proactive consultation to date, and its plan for further consultation in 2021, appears to be solely with the CI sectors identified as directly affected by the proposed regulations. We understand from the workshops that the Government views cybersecurity companies as key enablers of the proposed regime, rather than a key CI sector itself. We agree that ultimately the CI owners/operators themselves must ensure compliance with regulations. However, we encourage the Australian Government to also engage proactively with the cybersecurity community throughout this process, in addition to this public call for views on the consultation paper. We consider this important for four key reasons:

1) Cybersecurity is a fundamental pillar of the proposed regulatory framework and arguably one of the more complex subject matters.
2) Often the cybersecurity obligations imposed on CI sectors are directly passed onto or delegated to their cybersecurity vendors for implementation and appropriate action. This means the cybersecurity sector has first-hand experience of implementing cybersecurity requirements, such as standards, in the CI sector and can provide expertise on some of the common issues that can arise with respect to their implementation. For example, cybersecurity companies are regularly asked how they will support their financial sector customers' compliance with Australian Prudential Regulation Authority (APRA) regulation CPS 234. Under this regulation, companies are required to notify APRA of actual or *potential* compromises of information security. The reference to "potential" is not well defined and has resulted in significant confusion in the financial and cybersecurity industry.[2] Through engaging with cybersecurity companies, the Government can avoid replicating issues that have arisen in other contexts.
3) Cybersecurity companies often see threats affecting their customer base across the country and the world - including campaigns specifically directed at CI sectors.

[2] For example, is the release of a CVE classed as a "potential" compromise? What about a widespread phishing campaign that was blocked before affecting an organisation?

However, from the consultation paper it seems that public-private cyberthreat information sharing will focus solely on CI sectors. We would encourage the Australian Government to involve cybersecurity companies in any cyberthreat information sharing. We also note that cybersecurity companies can implement controls across their customer base to protect them against these threats not only after they have happened, but before.

4) Cybersecurity companies may be directly impacted by any Government directions and direct actions under the new regulatory framework. Given the current ambiguity about the new sectors to which CI regulation would be extended (see our comments below about the scope and implementation of direct action) it would be valuable for the Government to engage with the cybersecurity sector (and the ICT sector more broadly) to make sure its equities are understood and reflected.

Consultation Questions: Call for Views

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

Palo Alto Networks notes definitions for each of the sectors are yet to be provided, which makes it difficult to comment whether all functions are sufficiently captured.[3] However, we note that the list appears to reflect key sectors relevant to Australia's national and economic security. We see cybersecurity threats leveled across all sectors, including the mining and manufacturing sectors, as well as those sectors listed in the consultation paper.

2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

We note that the *Security of Critical Infrastructure Act 2018* defines "critical infrastructure" as the electricity, gas, water and maritime ports.[4] We agree with the Government that this definition does not reflect the range of sectors critical to Australia's national security and economic prosperity. In addition, the COVID-19 crisis has reshaped many governments' thinking on what sectors are considered "essential" or "critical". In the United States, definitions of critical infrastructure have evolved from being primarily 'sector'-based to 'function'-based, in the belief that this approach more accurately conveys the interconnectedness of modern supply chains. COVID-19 also has led governments to think

[3] For example, we assume that an institution like the ASX would fall under financial?
[4] *Security of Critical Infrastructure Act 2018*

about the essential nature of companies that support essential services; that is, companies which might otherwise not be considered essential or critical, but which supply components or provide manufacturing services for essential activities and therefore should be covered under the same essential services guidance. It is appropriate that the Australian Government take a fresh look at the sectors (or functions) that might now be considered critical, and reprioritise its cybersecurity efforts in terms of focus, protection and assistance (such as cyberthreat sharing, and other operational assistance).

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

All cyberattacks that occur in Australia, leverage Australian ISP and telco infrastructure to launch their attacks. As such, Palo Alto Networks believes the Government should prioritise strengthening our national defences via leveraging the telecommunication sector. As noted above in "general comments", the Government should encourage ISPs and Telcos to maintain constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cybersecurity threats within that traffic. This is not something Australian ISPs and telco providers currently deliver as a service but is a key mechanism to protect Australian CI sectors, and make Australia a less attractive target to cyber adversaries.

4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

We respond to this question by providing our observations about threats that all types of organisations are now facing, based on our experiences protecting tens of thousands of customers around the world from cyberattacks.

Globally, countless adversaries are willing to steal information, illegally make profits, and undermine their targets. Over the last decade the level of sophistication employed by adversaries (in particular, cybercriminals) has dramatically increased. While some criminals continue to compromise networks using publicly known vulnerabilities that have known mitigations, others are leveraging sophisticated attack tools to help find new exploits and automate and scale their attacks. Today, cybercriminals operate like a sophisticated business – they employ people, they have hierarchies and processes, and unfortunately they are

making a sizeable profit from their clandestine activities.

Palo Alto Networks threat intelligence team, Unit 42, confirms this trend. In an annual 2019 report on one Nigerian cybercriminal organisation, assigned the name "SilverTerrier", Unit 42 detailed their rapid expansion from just a few individuals experimenting with malware purchased online, to an organisation encompassing around 480 different actors and groups collectively producing more than 81,300 samples of malware linked to 2.1 million attacks worldwide.[5] The report also detailed that the frequency of SilverTerrier's attacks had dramatically increased. In 2018, there were an average of 34,039 attacks per month against Palo Alto Networks customer base. In 2019, this number climbed to an average of 92,739 per month – peaking at 245,637 attacks in the month of June 2019. While our customer base was protected against these attacks, the statistics demonstrated the widespread proliferation of cybercriminal activities.

An increase in cybercrime has also been experienced in Australia. In 2018, close to one in three Australians were victims of cyber-crime.[6] The Australian Cyber Security Centre (ACSC) receives a report of cyber-crime every ten minutes.[7] These attacks come at a significant cost to the Australian economy and our society. They also breed a lack of confidence and faith in online applications and can slow the adoption of digital transformation. It is estimated that cybercrime costs the Australian economy up to $1 billion per annum in direct costs alone and up to $17 billion in indirect costs.[8]

High profile incidents of cybercrime have exemplified the speed with which cyberthreats can propagate globally, how rapidly adversaries can adapt to security responses, and how easily a compromise can impact an organisation's core functions or services. In 2020, there has been increased reporting of cyber incidents affecting big Australian companies; a large Melbourne-based global logistics company has been hit twice by ransomware attacks, cyber incidents have also affected a government agency, resource company and a financial services company. On 19 June, Prime Minister Scott Morrison announced that Australian organisations, across a range of sectors and levels, were being targeted by a sophisticated state-based cyber actor.

[5] https://unit42.paloaltonetworks.com/silverterrier-2019-update/

[6] https://www.staysmartonline.gov.au/news/reverse-threat-cybercrime/stay-smart-online-week-2019

[7] https://www.zdnet.com/article/australians-are-reporting-cybercrime-activities-once-every-10-minutes/

[8] Australian Government, 2016 Cyber Security Strategy, https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

This is a trend that is likely to continue as the ACSC notes in their 2019-20 Annual Cyber Threat Report.[9] The report also identifies a trend that we are seeing - that ransomware and business email compromise continue to pose a significant threat to Australian Governments, business and individuals.

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

The TISN was designed as the Australian Government's primary engagement mechanism for business-government information sharing and resilience-building initiatives for CI. Led by the Critical Infrastructure Centre (CIC), the forum has historically had more of a focus on physical threats and foreign investment, in recognition that the cybersecurity expertise for Government resides in the ACSC.

It is important that within the Department of Home Affairs' proposed regulatory framework, the ACSC continues to be the main point of contact for industry on cyber - including with respect to information sharing and cyber resilience, cyber incident management and cyber exercises and/or playbooks. However, the CIC and the TISN can play an important role in providing a strategic and policy lens to Government activities. In particular, the TISN can play a role in:

- Convening industry - this avoids the duplication of effort across Government. For example, when the ACSC runs regular cyber exercises it can lean on the CIC and TISNs to convene the relevant industry members from that sector or across sectors.
- Running exercises based on scenarios that traverse all four key threats identified in the consultation paper (cyber, physical, personnel and supply chain protections).
- Sharing best practice - this forum can be leveraged as a mechanism to discuss best practice across the sector and sector groups.
- To host expert briefings on managing risk across cyber, physical, personnel and supply chain - including sharing of case studies.
- And providing a forum for reviewing and eliciting feedback on the regulatory framework - how it's working, challenges and gaps analysis.

Should the TISNs be leveraged to deliver on this mandate they will need to meet regularly and the supporting areas of CIC and ACSC will need to be adequately funded to achieve these objectives.

[9] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

The Government may also wish to consider whether the TISNs should also be expanded to reflect any additional sectors that the Department of Home Affairs adds to its CI definition based on this consultation. Government should also consider adding a TISN for the cybersecurity industry. In line with our “general comments'', we believe this consultation is critical to enhance the Government’s threat picture and improve our national resilience - a TISN could assist with this. At all times, best efforts should be made to avoid duplication of existing forums and functions. We note this answer is also relevant to question 8.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

We agree with the four key principles that underscore the positive security obligations (PSO) of:

1. Identify and understand risks
2. Mitigate risks to prevent incidents
3. Minimise the impact of realised incidents
4. Effective governance

However, we suggest that they are more cyclical in nature - in the sense that once an organisation has minimised the impact of a realised incident, they should undergo a deep dive as to why the risk manifested and how they can prevent it in future.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

As the *Cyber Security Strategy 2020* notes, ‘although the cyber skills and awareness of directors on the boards of Australia’s listed companies has been developed in recent years, there is opportunity for further development and support.’ The PSO, which are based on high level principles, will be important in creating cultural change among CI sectors and their boards - particularly when coupled with more frequent operational-level reporting between the CI and the Australian Government.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader

communication and engagement strategies of the regulator?

Palo Alto Networks would encourage the CIC and relevant regulators to:

1. Run extensive awareness campaigns. Specialised sectoral guidance and guidance on emerging security techniques will be useful—but only gets us halfway there. Organisations covered under the new regulatory framework need to know guidance exists and how to use it. The CIC and regulators should be directed to undertake extensive campaigns to raise awareness of its guidance and help organisations to leverage it. The CIC should work with states and territory Governments as well as industry stakeholders (i.e. via the TISN) in this effort, which should take various formats: workshops, webinars, and even the use of hands-on cyber exercises and cyber ranges. This should be produced and held in partnership with cybersecurity companies and national competent authorities charged with implementing the framework, including the ACSC.
2. With support from the ACSC, help organisations to validate their efforts and understand where they have gaps. Cybersecurity risk management is an ongoing process, and useful lessons will continue to be learned. Regulators and the ACSC should provide ongoing guidance and expertise to organisations about metrics of effective cybersecurity and how to validate their efforts.
3. Help identify smart goals. The ACSC should help organisations/sectors identify smart goals for cybersecurity risk management that are measurable, quantifiable, and time-bound.
4. Guide and empower organisations to embrace change and new technologies. In our experience, many organisations are worried about embracing new technologies. Practical and pragmatic guidance about how early adopters have successfully integrated state-of-the-art cybersecurity technologies would be useful, for example. This could be particularly helpful for utilities or other companies reliant on industrial control/SCADA systems. From our experience globally, for example, some energy companies are worried about harming their operational technology (OT) environments if they move too quickly to integrate new technologies.
5. Guide organisations to prioritise having confidence in their ICT vendors via their own procurement processes - looking at how securely a vendor develops its products and services should be the focus (in other words, the practices of the vendor), not the product/service itself.
6. Ensure appropriate enforcement of the framework. This will be important in order to gain the attention of the C-level executives.

7. The CIC and regulators should also provide clear guidance on how stakeholders can provide input to the process and voice any concerns, including clear timeframes for the framework's review.
8. Finally, in addition to guidance, a template for reporting to the Government as part of the PSO should be developed to ensure Government and Industry expectations are aligned as to the level of detail required.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

CI sectors are best placed to speak to this in more detail, although Palo Alto Networks notes there are a number of sectors which have regulators already addressing cybersecurity issues. These include APRA for the financial sector and the Australian Energy Market Operator for the energy sector. We note that whoever undertakes the regulatory role for these sectors must maintain close working relationships with the ACSC and Australian Signal Directorate - given they hold the cybersecurity expertise across Government. The Government should try and avoid a situation where regulators try to develop or deliver their own cybersecurity advice in isolation of the ACSC.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

Palo Alto Networks would recommend that the Government invest in upskilling the regulators on cybersecurity issues and risks via target training and briefings. This should include briefings from the ACSC as well as cybersecurity companies - particularly those that work closely with a particular CI sector(s).

19. How can the Government better support critical infrastructure in managing their security risks?

The Government should promote greater public-private sector voluntary sharing of cyberthreat information. The Australian Government, namely the ACSC, has acknowledged the value of voluntary cyberthreat information sharing in understanding the threats, protecting information and networks, and preventing successful cyberattacks. The ACSC is

continuing to build out these capabilities as part of the Cyber Enhanced Situational Awareness and Response (CESAR) program.[10] In support of this, the Australian Government should:

- educate Australian organisations as to the value of voluntarily sharing cyberthreat information to prevent attacks;
- promote the expansion of information sharing organisations across industry sectors; and
- encourage all participants to increase the maturity level and effectiveness of threat sharing, and make it more operational and actionable, via automation and real-time feedback loops.

Additionally, and as noted above, the Australian Government should also harden our national defence by working with ISPs and Telcos to be able to detect and stop in real time cybersecurity threats within that traffic. This would significantly reduce the volume of malicious traffic targeting CI sectors and make Australia a less attractive target for cybercriminals.

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

Government and industry both bring unique and complementary capabilities when it comes to cyberthreat intelligence. By their nature, Governments have a unique vantage that allows them to holistically evaluate and prioritise the most significant risks to the critical sectors, functions, and organisation that underpin their national security, public safety and economic stability. In this way, Governments can effectively task industry to prioritise their threat intelligence analysis efforts to align with the most significant national and international risks. Industry, particularly cybersecurity companies, are well suited to use their visibility across critical infrastructure sector networks globally to enrich the Government's understanding of shared adversary's malicious cyber activities against these priority targets.

To more effectively collaborate on an operational level to address real-world cybersecurity challenges, the Australian Government should look to more freely share declassified real time cyberthreat information with industry. This will tool industry with the information required to detect and prevent threats. The Government may also wish to establish a program in which private sector experts can work alongside on a part-time basis ACSC

[10] https://www.pm.gov.au/media/nations-largest-ever-investment-cyber-security

experts at a declassified level. One model is the UK's Industry 100 (or i100), set up by the National Cyber Security Centre (NCSC) in 2016.[11] Under the i100, declassified intelligence is provided to i100 members who enrich it with their own data, collaborate, and investigate. The outcomes include holistic reports focusing on specific threats/actors or sectors, providing an improved view of the landscape and indicating immediate actions to improve organisations' security postures. Both the NCSC and industry benefit. The NCSC typically gains many more leads and data points, allowing for further analysis. Depending on the nature or the traffic light protocol (TLP) rating of the information, industry many times can enrich its data with the findings from joint initiatives to in turn help its research and customers. In short, this is a mutually beneficial model that allows for scalability.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

Palo Alto Networks, as a matter of principle, collaborates with trusted government partners around the world, including the ACSC, to share technical threat intelligence because cybersecurity is a shared global challenge. We remain committed to doing so on a voluntary and ongoing basis. We've also taken a leading role in organising better sharing among the private sector, by founding the Cyber Threat Alliance, the cybersecurity industry's first automated information sharing organisation.[12]

These partnerships often result in real world actions that tangibly reduce the global cyberthreat. Over the last several years, our threat intelligence team has partnered closely with law enforcement entities worldwide on multiple cybercrime and cyberespionage cases. We've helped law enforcement identify hundreds of malicious actors across multiple campaigns, leading to the arrest and prosecution of numerous cyber criminals.

27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

Palo Alto Networks recommends that the Government draw on the collective and lived experience of the private sector in developing playbooks - including the experiences of cybersecurity companies. We would like to discuss opportunities to share playbooks across

[11] https://www.ncsc.gov.uk/information/industry-100
[12] https://www.cyberthreatalliance.org/

industry and government cybersecurity entities.

28. What safeguards or assurances would you expect to see for information provided to Government?

Palo Alto Networks recommends that companies be able to share threat intelligence anonymously, in real time and that they be able to tag information for the attention of certain audiences. The Government should leverage, and educate CI sector contributors, on the TLP and provide assurances that under no circumstances will they share information beyond the terms agreed, without the explicit consent of the original source of information. Threat information shared voluntarily with the Government should be used only for cybersecurity purposes (not regulatory purposes, for example), and the Government should ensure the proper privacy protections are in place.[13] The Government may also need to provide assurances that information shared will not be subject to Freedom of Information-type requests. Failure to do so will likely affect the willingness of many companies to share information, for fear that it may make its way into the public domain.

Questions 29-36: Entity and Government Action

The third section of the consultation paper addresses the ability of the Government to either issue directions to CI entities (directions), or to take direct action itself in the national interest (direct action). The latter is articulated below.

> *In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national interest. These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow Government to assist entities take technical action to defend and protect their networks and systems, and provide advice on mitigating damage, restoring services and remediation (p.29).*

We note that questions 29 to 36 address a number of questions that are a matter for the Government. However, we would make the following observations:

[13] Australia may want to look at the U.S. Cybersecurity Act of 2015 (CSA)l. Among other topics, CSA focused on cyberthreat information sharing; it established clear legal authority and liability protections for the appropriate voluntary sharing of certain types of cyberthreat information between private sector entities, and for private sector entities who share cyber threat information under certain guidelines with the U.S. Government. The Act also provided guiding principles on privacy issues.

Directions

1) Requests or directions should be issued to the CI organisation (i.e. individual business), not to the organisation's cybersecurity provider. This due to the fact that the CI organisation is best placed to understand which systems are being threatened, and how this impacts their business operations.

Direct Action

2) The Government should apply a high threshold for when it can take direct action, with a strong preference in favour of directions to entities in the first instance.
3) There are difficulties and limitations of direct action. In particular, it would be very difficult for a Government officer to defend an organisation's networks where they do not have an intimate understanding of the organisation's systems. There is also a chance that they may cause further or unforeseen damage to the company's ICT infrastructure as a result of their unfamiliarity. We recommend all direct action be undertaken in close partnership with the CI's cybersecurity team or provider.
4) All direct action should be tightly defined and controlled - articulating what the Government and its officials can do, for how long and why. This should also specify that Commonwealth officers cannot conduct offensive cyber activities from within private sector infrastructure. The execution of the direct action power should be reasonable and proportionate.
5) Direct action should require sign off at the highest levels of Government (i.e. at the Ministerial level). We would also suggest sign off should be from both the Defence and Home Affairs portfolios. This is particularly relevant in the cyber context, as operations and policy currently sit across the two portfolios. It is reasonable to expect that in making a decision on direct action that the Ministers from both portfolios are agreed on its merits and necessity.
6) Oversight of these new arrangements will be important to maintain public trust and confidence. It will also be important that oversight is at the lowest security classification possible, given these actions directly impacting CI whose operations are outside of a classified environment and should be open to some degree of public debate.
7) Companies should have an appropriate avenue for redress with respect to directions or direct action to ensure the continued efficiency, transparency and accountability of the process.
8) It will be important to clarify whether immunities are afforded to CI sector subcontractors. For example, whether immunities would apply to a cybersecurity company that takes actions on behalf of their CI client at the direction of the

Government. It should also address liabilities and immunities in the event that a government directed change adversely impacts other customers or causes the entity or their providers financial losses.

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 [redacted] and Sean Duca, chief security officer, Asia Pacific & Japan, at [redacted].

About Palo Alto Networks

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

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