27 November 2020

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

Re: Submission - Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Palo Alto Networks appreciates the opportunity to provide input to the Department of Home Affairs' call for views on the *Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill).* We congratulate the Australian Government on its leadership on cyber security and critical infrastructure (CI) matters to date.

Palo Alto Networks is the largest cyber security company in the world. Palo Alto Networks secures the networks and information of more than 77,000 enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cyber security posture. We work with some of the world's largest organisations across all industry verticals, including in many CI sectors. We combine our knowledge from working with customers and governments across the world to directly inform our response.

On 16 September, we provided comments to the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* which we have attached for reference. Below we comment on the Bill.

General Comments

Palo Alto Networks supports the Government's commitment to taking further action to improve the cyber security 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 Bill. We look forward to working with the Government to co-design the sector-specific requirements to be included in the CI Risks Management Program (RMP) - particularly with respect to cyber and supply chain security standards. Before addressing the specifics of the Bill, we have the following observations and recommendations.

Recommendation: The Bill Should Consider Supply Chain Declarations or Directives

As it currently stands, Part 3A of the Bill appears to provide the Minister for Home Affairs the power to issue an action direction in the event of a 'cyber security incident' as defined in

section 12M. However, the Government may also wish to consider having the ability to issue directions to CI based on serious supply chain security concerns. For example, the U.S. Government has issued these kind of binding directions - most notably when the Department of Homeland Security (DHS), in consultation with interagency partners, determined that the risks presented by Kaspersky-branded products justify issuance of a binding operational directive to remove and discontinue present and future use of all Kaspersky-branded products within 60 days.[1] These directives are not necessarily made in response to a 'cyber security incident' but rather, may relate to a supply chain issue or concern, such as the tampering of certain products (i.e. hardware or software) where the effect may or may not have been realised or necessarily be imminent. Depending on the definitions of key terms under section 12M and section 35AB(1), the Bill may not provide a means for the Government to communicate and direct public and private sector organisations not to use certain products due to supply chain security concerns. Such a directive should provide advanced notice to the affected company or company in question, to enable them to either remediate the issue or afford them a right of reply (where appropriate).

Recommendation: Appropriately Resource the Department of Home Affairs

Under the proposed regulations, the Department of Home Affairs (DHA) will be the de-facto regulator for a number of sectors, including the Communications, Food and Grocery, Education and Research, Health and Medical, Space, Water and Sewerage sectors. This is a significant increase in the scope of the Department's role and should be matched equally with funding and resources. We also note that given cyber security expertise in the Government resides in the Australian Cyber Security Center (ACSC), ACSC and DHA should work seamlessly together to ensure alignment and appropriateness of messages.

Recommendation: Complement Legislation with Other Activities to Support Industry

As per our September submission, Palo Alto Networks would encourage the DHA and relevant regulators to run extensive awareness campaigns on the new regulatory regime. Organisations covered under the new regulatory framework need to know what guidance exists and how to use it.

Specific Comments: Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill

PART 1 — General Amendments

Remove Data Storage or Processing as a CI Sector

[1] https://cyber.dhs.gov/bod/17-01/

Data storage and processing has taken on an increasingly important role across all economies. However, governments have largely avoided defining cloud and/or data processing/data storage as a separate CI sector due to its cross-cutting nature, and the fact that so many other sectors are dependent on cloud and/or data processing/storage as horizontal enablers of these other sectors. We encourage the Government to remove 'Data Storage or Processing' as a CI sector on the following basis:

1) Definition of 'Data Storage or Processing' is Too Broad. From our reading of the Bill this sector includes everything from enterprise data centers to cloud services to all manner of services delivered via the cloud.

   Section 12 F of the Bill provides that an asset is a 'critical data storage or processing asset' if it is owned or operated by an entity that is a data storage or processing provider and it is used wholly or primarily in connection with a data storage or processing service that is provided on a commercial basis to an end-user that is:

   i. The Government (Commonwealth, State or Territory); or
   ii. The responsible entity for a CI asset; and the service relates to business critical data.

   However, a number of these terms are not defined and are open to a broad and problematic interpretation. In particular:

   - The scope of data storage or processing is unclear, as 'data processing service' is not a defined term in section 5 of the Bill.
   - The words 'wholly' and 'primarily' are not defined in the Bill.
   - It is unclear what the Government considers 'relates to' in the context of business critical data. For example, is it the intent that a cyber security product delivered via the cloud that, *inter alia,* protects an entity's business critical data would 'relate' to business critical data?
   - Finally, it is unclear what the Government's current review of the *Privacy Act 1988* will have on the scope of the proposed definition in this Bill of 'business critical data'. We note that under this review, the definition of 'personal information' may be expanded to include IP addresses and other technical data.

2) Conflation of Cloud Services Providers (CSPs) and Data Centers. We note that while CSPs may leverage data centers, these entities may have different risk profiles. Thus, an approach to security that may be appropriate for an enterprise data center may not be appropriate for a CSP. Conflating the two sectors negates the risk-based approach to CI protection (the aim of the Bill).

3) Confusion with Sector-Specific Rules. It is unclear how sector-specific CI rules (for example, rules in the energy sector, telecom sector, or financial sector), would interact with the positive security obligations (PSOs) for 'Data Storage or Processing' providers. The Government may wish to consider managing the security risks associated with CSPs in an analogous way to how other 'horizontal' risks are managed (cyber, supply chain, personnel, physical security).

PART 2 — Register of Critical Infrastructure Assets

Positive Security Obligations (PSO) Activation

Palo Alto Networks supports the intent of the PSOs which aims to improve our national resilience and create cultural change across the public and private sectors with respect to cyber security and supply chain risk management practices.

We note the PSOs will contain a number of elements but will only apply in circumstances where the Minister for Home Affairs has made a rule turning on the specific obligation for a particular CI asset. However, the rationale as to when and why such a determination is made is not clear in either the Bill or the Explanatory Document (ED). It is also unclear how organisations will be notified of determinations that they are a CI asset. We believe that organisations should be given clarity as to how these decisions to 'switch on' reporting obligations are made.

Security of Information Disclosed Under PSOs

We welcome the Government's recognition at paragraph 266 of the ED, that any information provided to the Government's register of CI assets could potentially include business confidential or sensitive information, and as such will be recognised and considered as protected information under existing law and handled as such. However, we would encourage this to apply to all information provided under the PSOs (including the annual updates of the RMPs, for example).

We also note that the Government should provide assurances that information shared under Part 2B 'notification of cyber security incidents' should be shielded from Freedom of Information-type requests. Failure to do so may affect information sharing as companies risk sensitive security information making its way into the public domain.

Phased Implementation After Finalisation of Standards

As per paragraph 274 of the ED, the Government has permitted a 6-month period to allow companies time to bring business processes in line with their PSOs. While we welcome the

delayed commencement of obligations, we would suggest that more time is required for companies to appropriately budget for and amend company policies to comply with the proposed regime.[2] We also note that the sector-specific standards are yet to be co-designed with industry and that any transition period should commence only once the sector-specific standards have been developed and agreed to.

Part 2A - Critical Infrastructure Risks Management Programs (RMP)

Palo Alto Networks welcomes the establishment of a clear and consolidated legislative framework for CI assets to address the risks associated with a range of security issues, such as cyber and supply chain security. However, we note that any legislative obligation will be more successful as a flexible, outcome-oriented framework rather than a static checklist requirement.

We appreciate that the Bill sets out the overarching obligations for the RMP with more detailed sector-specific requirements to be contained in the rules. However, this makes it difficult to assess the regime as a whole, without access to those rules and their method of formulation. It is important that co-design processes be rigorous, genuine and leverage existing international standards where appropriate. At this stage we have the following observations.

<u>Consider Engagement on RMPs to Ensure Consistency</u>

We note that much of the detail within the RMPs is left to the discretion of the CI asset in recognition that the individual organisations are best placed to understand their own unique cyber security risks. At the same time, the Bill does not afford DHA and the regulators authority to collaborate with CI assets on the RMPs. We suggest that DHA and the regulators should (at least initially) take a more active role in driving consistency across sectors in terms of these RMPs, such as defining opportunities for CI assets to voluntarily collaborate with DHA on the RMP; defining a standard period of time for updating RMPs; or clarifying what will happen if RMP reporting does not meet DHA standards.

<u>Undertake Consultations with Cyber Security Companies on Sector-Specific Requirements</u>

As per our September submission, we encourage the Government to engage proactively with the cyber security community to determine the requisite cyber security standards for each of the CI assets to be contained in the rules (in addition to consultation with each affected sector). Often the cyber security obligations imposed on organisations are directly passed onto or delegated to their cyber security vendors for implementation and appropriate action. This means the cyber security sector has first-hand experience of implementing cyber

[2] We note here that company budgeting processes occur usually 12-18 months in advance. We understand that GDPR afforded companies a period of 2 years to implement procedures.

security 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.

Sector -Specific Requirements Should Draw on Existing International Standards

In developing the sector-specific requirements, the Government should work with industry to identify and draw on existing consensus-based international standards as a first choice before commencing development of any new, Australia-specific standards. This can ensure that the required standards do not introduce unnecessary complexity into the risk mitigation activities of CI assets. Unfortunately, some governments and multilateral organisations are increasingly seeking to develop new ICT standards (when effective ones already exist) 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. In addition to the security benefits of interoperability, such an approach will also avoid the establishment of unnecessary barriers to trade, which may have an adverse effect on Australia's economy.

Rules Must Maintain Pace with Technological Change

It will be important that the Government work with its stakeholders to ensure that the rules underpinning the RMPs keep pace with technological advances and the threat landscape. For example, we note at the ED at paragraph 297 calls out AEMO's Australia Energy Sector Cyber Security Framework. However, this framework released in 2018 has struggled to keep pace with technology changes and security developments in the energy sector. For example, the Framework does not address emerging security issues associated with distributed energy resources and microgrids, which have seen an increase in the number of market participants (with varying levels of cyber maturity), remote connectivity and reliance on automation.

PART 2B - Notification of Cyber Security Incidents

We understand that the Government is interested in knowing about cyber security incidents so as to assist impacted CI organisations and also leverage lessons learned to prevent additional and future incidents. However, we have the following observations:

Timeframes for Cyber Security Reporting

The timelines of 12-hours and 24-hours for reporting a 'Critical Cyber Security Incident' and 'Other Cyber Security Incidents', respectively, are unnecessarily short. This requirement injects additional complexity at a time when CI assets are faced with the difficult task of responding to a cyber incident. It also greatly increases the likelihood that the CI asset will report inaccurate or inadequately contextualised information that might be shared further

with the Government and potentially other impacted entities, but that will not be helpful. We also note that the full extent and impact of a cyber security incident may not be known or well understood within 12 hours of it being realised, making it difficult for an organisation to determine whether it is a 'critical' or 'other' cyber security incident within the timeframes. We strongly recommend that the Government replace arbitrary timelines with a requirement for companies to report 'as soon as reasonably practicable' or 'without undue delay'.

Critical Cyber Security Incident

The definition and criteria for a 'critical cyber security incident' is not defined in the Bill. Of note the term 'significant impact' in section 30BC(1)(b)(ii) is not defined. The ED provides some commentary on this at paragraph 319, noting that determining whether an incident is having a significant impact on the availability of the asset will be a 'matter of judgment for the responsible entity' and that the threshold has been left 'internationally undefined as the significance of an impact on the availability of an asset will vary radically between assets'. It also notes that it is 'not intended that day-to-day incidents...should be reported.' While this guidance is helpful, it does leave many organisations guessing what constitutes a 'significant impact' on the availability of an asset. We would recommend that the Government provide further guidance on this threshold.

Other Cyber Security Incidents

The threshold for reporting 'other cyber security incidents' appears to be too low and the outcome of this provision will likely be an overreporting to the Commonwealth of incidents that may or may not be actionable. Of note:

- Section 30BD(1)(b) sees the introduction of the requirement to report where not only has an incident occurred, or is occurring but also, where a cyber security incident is 'imminent'. The term 'imminent ' is not defined in the Bill or the ED. For example, does this refer to a scenario where there is a disclosed vulnerability but the organisation is in the process of patching their systems? Does this require companies to report on attempted incidents?
- The Bill also notes that the incident must have also 'had, is having or is *likely* to have a relevant impact on the asset'. It is unclear how a CI asset can determine whether an incident is *likely* to have a relevant impact - as 'likely' remains undefined and guidance on the parameters here is missing.

- The ED goes further and explains that 'by contrast to a critical cyber security incident, this obligation relates to *any* impact on availability (irrespective of significantly) alongside other forms of impact'.

Reading section 30BD as whole, the reporting threshold is too low and will likely result in the Commonwealth being overwhelmed by receiving thousands of reports (if not more) per day, undermining the Government's ability to provide timely and actionable advice to the CI assets. The reporting threshold also will unnecessarily burden CI entities who will likely err on the side of reporting too much (or will have to spend time determining if an incident is imminent or likely to impact an asset) - which will divert information security teams' attention and limited security resources away from the essential tasks of actually examining and remediating an incident/ securing their systems.

PART 3A - Responding to Cyber Security Incidents

We welcome the decision to elevate a number of the powers granted in Part 3A to the Ministerial level. In particular, we welcome the additional levels of sign off from the Defence Minister and the Prime Minister with respect to intervention requests. However, we have some concerns with the proposed regime, which are articulated below.

Part 3A to Consider Commercial Feasibility and Multi-Tenant Products

The current process established under Part 3A, which permits the Minister to subject CI assets to 'Information Gathering Directions', 'Action Directions' and 'Intervention Requests' does not take into account the commercial feasibility of requests, nor does it take into account multi-tenant products (which affect all users at once, rather than being able to make isolated changes to the system.) We therefore recommend the Government articulate, in either the Bill or the ED, that it will pay due regard to the commercial feasibility of its request and the impact of its request on multi-tenant products in exercising its powers under Part 3A. We also recommend that a clear and expeditious appeals process be established in the event that the Minister makes a request that is not commercially feasible and would place a party into a burdensome position for the sake of compliance.

Independent Arbiter of Action Directions and Intervention Requests

Section 35AB, addresses the requirements by which the Minister can authorise both 'Action Directions' as well as 'Intervention Requests'. At a high level, both sections 35AB(7) and 35AB(10) note that the Minister must not authorise these actions unless the Minister is satisfied that 'the specific entity is unwilling or unable to take all reasonable steps to resolve the incident' where the direction is reasonably necessary and technically feasible. We note

that section 35AB(10) [Intervention Requests] has additional requirements that an 'Action Direction' have been issued and that the intervention request is proportionate to the incident.

It is reasonably foreseeable that the Government and Industry may disagree as to the best course of action in response to a cyber security incident. In these situations this may be interpreted by the Government as an 'unwillingness' to take 'all reasonable steps to resolve the incident' on the part of the CI asset, but there may be a legitimate reason the CI asset chose another action. As such, we believe 'Action Directions' and 'Intervention Requests' should be subject to an independent and expeditious assessment, that can be triggered by the appeal of the entity or CI asset in question, should that entity believe in good faith that it possesses the willingness and ability to address cyber threats, but disagrees with the Government's intended risk-mitigation strategy or course of action. This appeal process should also be applicable where Industry may disagree that an 'Intervention Request' is a 'proportionate response' as per section 35AB(10)(e).

Given the stark penalties for failing to comply requests under Part 3A (i.e. up to 2 yrs imprisonment or $31,500) and limited rights of appeal (i.e. there is no judicial review under the *Administrative Decisions (Judicial Review) Act 1977*(Cth)), we believe than an independent appeals process is critically important to the success of this new regulation.

Inspector General for Intelligence and Security (IGIS) Oversight

Palo Alto Networks suggests that IGIS is not an appropriate oversight mechanism for Part 3A powers. IGIS has a mandate to oversee our intelligence agencies and its operations are highly classified. Oversight here should be open and transparent (within reason) in order to maintain public trust and confidence. It will also be important that oversight is at the lowest security classification possible, given these actions directly impact CI assets whose operations are in the public domain.

Conclusion

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 cyber security leader, is shaping the cloud-centric future

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

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