1 March 2022

Parliamentary Joint Committee on Intelligence and Security
Committee Secretariat
PO Box 6021
Australian Parliament House
Canberra, ACT, 2600

RE: Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Palo Alto Networks appreciates the opportunity to provide a submission in response to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry regarding the *Security Legislation Amendment (Critical Infrastructure) Bill 2022* (herein 'the Bill').

Palo Alto Networks is the global cyber security leader, securing the networks and information of enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cyber security posture. We work with some of the world's largest organisations across all industry verticals, including in many critical infrastructure (CI) sectors.

We congratulate the Australian Government for its leadership on cyber security and CI matters to date. We also appreciate the Parliament's continued interest in these critical infrastructure reforms and its willingness to engage stakeholders in the development of this Bill via a public consultation process.

Palo Alto Networks has been actively engaged in the development of the Government's Critical Infrastructure Reforms. We have submitted responses to the previous PJCIS review on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, we also appeared before the PJCIS as part of its public hearings in July 2021. We appreciate the PJCIS's engagement. At the Departmental level, we responded to the call for views on the two preliminary documents that have informed the full scope of these reforms: 1) the Department of Home Affairs (DHA)'s *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* (comments dated 16 September 2020) and 2) DHA's *Exposure Draft* of the Bill itself (comments dated 27 November 2020). Before addressing the PJCIS's current scope of inquiry, we would like to reiterate some of our key concerns with the 2021 amendments made to the *Security of Critical Infrastructure Act 2018* (herein the Legislation).

Security Legislation Amendment (Critical Infrastructure) Bill 2021

We acknowledge and appreciate that the 2021 amendments made to the Legislation falls outside the scope of this PJCIS process. However, we would like to reiterate our concerns that:

1. *Cyber incident notification timeframes remain too rigid.* Under the Legislation, 'critical cyber security incidents' must be reported within 12 hours of the responsible entity becoming aware

of the event. We note the changes recommended, and subsequently made to the Legislation, which provide that where the first report is given orally within 12 hours, then a written report must be provided within 84 hours of that first report. While we appreciate amendments to the timeframes, we still believe the requirement to notify within 12 hours is too rigid and 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, which could complicate or delay mitigation efforts. 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 continue to recommend that the Government replace arbitrary timelines with a requirement for companies to report 'as soon as reasonably practicable' or 'without undue delay'. This would ensure the Government has access to accurate and actionable intelligence. We also encourage the Government to ensure that these reporting obligations are aligned with and consider other incident obligations already levelled on industry, such as those under *the Privacy Act 1988* (Privacy Act) and the proposed ransomware reporting requirements.

2. *Continued concern about the scope of 'other' cyber security incident reporting requirements.* Under the Legislation an entity is required to notify when the entity becomes aware not only if an incident occurred, or is occurring but also, where a cyber security incident is 'imminent'. This reporting threshold is concurrently overly broad and unclear and could result in the Government being overwhelmed by receiving thousands of reports (if not more) per day, particularly if there is uncertainty among covered companies of their obligations to report incidents that have not yet happened. Overreporting to the Government of incidents that may or may not be relevant may serve to undermine 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.
3. *Ongoing concern about the application of Part 3A 'Government Assistance Measures'.* While we understand from the Government that Part 3A powers are a 'measure of last resort', we remain concerned about the lack of a clear legislative appeal right for companies that may be subject to these powers. We also remain concerned about the commercial feasibility of these responses, particularly for multi-tenant cloud products (where changes can affect all users at once, rather than being able to make isolated changes to the system). Thus, we continue to recommend that a clear and expeditious appeals process be established in the event that the Government makes a request that is not commercially feasible and would place a party into a burdensome position for the sake of compliance.

We note that some of the above concerns could be addressed via the publication of guidance materials

on how the Government intends to operalise the Legislation. In particular, we would welcome guidance about the incident reporting obligations to further articulate what the government intends to capture, and to define what they consider actionable threats, as opposed to common activities such as adversaries conducting vulnerability scanning of networks and systems. We would encourage the Government to develop these materials in close collaboration with industry. Palo Alto Networks stands ready to support the Government with the development of these materials.

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Given the short timeframe necessitated for the review, the PJCIS has asked specific questions as part of the submission process. We have addressed one of these below.

Key Questions: What are our Five Key Themes of Feedback on the Bill?

1. **Concern Re: Division 5 - Access to System Information**

   This Division appears to grant the Government the ability to continually access System of National Significance (SoNS) system information with few checks and balances on this power. The Division also fails to articulate criteria or standards the Government could consider for mandating this reporting, nor does it specify - or provide any assurances as to - how the data collected would be used.

   Lack of Guardrails for Powers Under Subdivision A—System Information Reporting Notices

   This subdivision establishes far-reaching powers which see the Secretary able to request SoNS entities to provide both 'system information periodic reporting' and 'system information event-based reporting'. According to the Explanatory Memorandum (EM), [s]ystem information is data generated about a system for the purposes of security, diagnostic monitoring or audit, such as network logs, system telemetry and event logs, alerts, netflow and other aggregate or metadata that provide visibility of malicious activity occurring within the normal functioning of a computer network.' Although this excludes personal information captured under the Privacy Act, this information is sensitive in nature and these powers are substantial.

   We are concerned that Bill does not provide for the appropriate checks, balances and justification of Subdivision A powers. Section 30DE sets out the maximum time frame of 12 months for which a system information periodic reporting notice, or a system information event-based reporting notice, can be in force. We believe given the invasive, and potentially disruptive and costly nature of these powers, that the maximum duration for these notices should be shortened. These notices should be regularly reviewed to see if they are still necessary, proportionate and reasonable, and impacted companies should have some avenue of redress to request reconsideration of these requirements. Finally, the Government should

specify how the collected data will be used and provide an undertaking that it will not be used for other purposes.

We also note that there are no limitations on this power. Section 30DC states that just because one of these requests are in force, this does not prevent the Secretary from giving a fresh notice that is in the same, or substantially the same, terms as the original notice and that new notice can come into force immediately after the expiry of the original notice. There is potential that this lack of specifically articulated criteria for extending or issuing new information requests further deprives impacted industry members of the ability to have meaningful input to this exercise of governmental power.

Finally, we note that section 30DC also provides the Secretary powers to direct a SoNS entity to provide reporting of system information if a particular kind of event occurs - where 'particular kind of event' remains undefined. We would appreciate further guidance on this term and its definition.

In summary, we would recommend that the Government reconsider these provisions and create stronger checks and balances on the execution of these powers.

Recommendation: Amend the Bill to improve the guardrails for the execution of powers under 'Subdivision A—System Information Reporting Notices.'

Unfettered Powers of Subdivision B—System Information Software

We are concerned by Section 30DJ which provides that the Secretary may require a relevant SoNS entity to install and maintain a specified computer program to collect and record system information to be transmitted to the Australian Signals Directorate (ASD). We appreciate this is a 'provision of last resort' however, we do not think it appropriate that the Australian Government and its intelligence agencies should be able to force private enterprises to install intrusive software on their networks.

The installation of software for monitoring purposes could expose sensitive data from cyber security services and products, that in some cases may be unrelated to the scope and purview of the underlying information request, and pass it through to the ASD. This potentially unfettered access, without necessary contextualisation from the entity, could be misinterpreted and cause broader operational disruptions. Additionally, this level of access could expose information and systems from other entities in a provider's supply chain, which could complicate contractual duties and other standards of care between providers. We note that this may also expose the Government to liability for any adverse impacts arising from the installation of this software.

Not only is this power intrusive, it also may weaken an organisation's security posture. The installation of what constitutes third-party software has the potential to create vulnerabilities

that could adversely impact the security of a SoNS entity as well as, by default, Government systems and client systems.

Similar to the above comments, we note that entities can be required to provide information to the ASD via this monitoring software for a period of up to 12 months - which we believe is too long a period without undergoing a review of whether the request is still relevant, necessary or proportionate. We also note that these powers are not limited - meaning that at the same time as asking a SoNS entity to install this monitoring software, the Secretary could also ask the same SoNS entity to provide one or both 'system information periodic reporting' and 'system information event-based reporting' - all of which could be issued on a rolling basis. This could see a SoNS entity subjected to heavy and intrusive surveillance of their networks for an extended period of time without review or appeal rights.

The mandatory provision for installation of government software also has the potential to adversely affect business interests and investment, as clients may doubt the system integrity of companies operating in Australia (as they may have this software on their systems). For the above reasons, we recommend that Subdivision B be removed in its entirety from the Bill.

Recommendation: Remove 'Subdivision B—System Information Software' in its entirety from the Bill.

2. **A Review or Appeal Mechanism is Needed**

We are concerned by the exclusion of merits review for section 30CB, other Part 2C decisions and decisions to declare a system of national significance. Given the potentially unprecedented and broad nature of these powers, it is critical that entities have an appeal mechanism available to them should they disagree with a Government decision or request.

While we acknowledge that the: 'Minister's decision under section 52B can only be made by the Minister personally, and there is no statutory power of delegation of the Minister's powers under the SOCI Act. It is further noted that judicial review, including review under the Administrative Decisions (Judicial Review) Act 1997, is available in relation to such decisions.'[1] However a vast number of the powers outlined in this Bill are granted to the Secretary and the ASD, and may not be subject to review or appeal processes. Given a number of these powers are potentially unprecedented, the basis on which they are used should be subject to review, and impacted private sector entities should have the ability to inform the use of these potentially extensive powers.

We also note that these powers (and the lack of review or appeal rights held by affected entities) may adversely affect the attractiveness of Australia as a market for investment but also, may adversely impact the ability of Australian businesses to grow internationally. In accordance with Australian values and

[1] Explanatory Memorandum

principles, we would encourage the Australian Government to reconsider this exclusion. The current exclusions of a merits review could set a precedent that if adopted by other countries, could negatively impact Australians and the technologies they rely upon. We continue to recommend providing a legislated, independent and expeditious appeals process of government powers granted under this Bill and the Legislation more broadly.

Recommendation: Amend the Bill to provide for a legislated, independent and expeditious appeal process.

3. Concern Over Vulnerability Assessments by 'Designated Officer'

Section 30CW of the Bill outlines the circumstances in which a 'designated officer' may undertake a vulnerability assessment of a SoNS. A designated officer for the Bill's purpose means an APS employee of the Department or a staff member of ASD who is appointed by the Secretary. As per the EM, 'a vulnerability assessment involves identifying potential points of weakness or gaps in the systems and networks that are relevant to the continued operation, functionality, and security of systems of national significance. An assessment may include (but is not limited to) vulnerability scanning or testing.' A vulnerability assessment direction can be made by the Secretary where the 'entity is incapable or unwilling to undertake the assessment'.

A vulnerability assessment is an incredibly invasive process and it is reasonably foreseeable that Government and industry may disagree as to the best timing and focus of a vulnerability assessment, as well as who should undertake this assessment. In these situations, a disagreement may be interpreted by the Government as an 'unwillingness' to undertake the assessment. Given the nature of these powers and the associated severity of penalties, in line with the above comments, SoNS entities should be able to appeal the decision by the Secretary to order an assessment of their networks by a member ASD.

We also note that the designated officer must provide a copy of the report to the Secretary within 30 days of completing the assessment. We would encourage the Government to provide organisations with a right of reply to this report - whereby organisations can provide greater context to the assessment or outline their plans for remediating vulnerabilities across their network.

Recommendation: In addition to providing review and appeal rights, amend the Bill to provide SoNS entities a right of reply where they are subject to a vulnerability assessment in accordance with section 30CW.

4. Consideration of Commercial, Technical and Practical Feasibility

Before imposing various obligations under Part 2C of the Bill, the Secretary is required to have regard to:

- the costs that are likely to be occurred by the entity in complying with the notice; and
- the reasonableness and proportionality of the requirement in the notice; and

- such other matters (if any) as the Secretary considers relevant.

The EM notes in several places that 'other matters' the Secretary may consider relevant include 'any international trade obligations that apply, whether the entity is, or has been, subject to any other enhanced cyber security obligation, and whether the entity is subject to another regulatory regime under Commonwealth, State or Territory law that is similar.'

We would recommend that the Bill be amended to ensure that the Secretary has due regard to the commercial, technical and practical feasibility when exercising powers under the Bill. This should take into account not only the technical feasibility or challenges of implementing an approach but ensure that a company cannot be forced to breach a contractual relationship or be non-compliant with the laws of another jurisdiction in order to comply with the Australian Government's request.

Recommendation: Amend the Bill to ensure that the Secretary must have due regard to the commercial, technical and practical feasibility when exercising powers under the Bill.

5. Appropriate Classification and Handling of Information

Under this Bill the Government can collect an array of highly sensitive information on a SoNS entity - for example, cyber vulnerability assessments and incident response plans would provide information that is of interest to a range of adversaries, particularly in aggregate. We would encourage the Australian Government to appropriately classify and handle this information on a 'need to know basis and provide assurances to SoNS entities of this undertaking. We would also encourage the Government to provide assurances that information shared as part of these requirements is shielded from Freedom of Information (FOI) -type requests. Failure to do so may affect information sharing as companies would fear risking sensitive security information making its way into the public domain.

Recommendation: Amend the Bill to ensure that information collected by Government in accordance with the Bill is:

- **Appropriately classified and handled by Government on a 'need to know' basis; and**
- **Is not subject to the FOI-type requests.**

Other Points

Notification of SoNS Status to Key Providers

Under the conditions set out by the Bill, a SoNS-declared entity is prevented from disclosing to third parties that they have received such a designation. We recommend that the Bill be amended to permit entities to disclose SoNS declarations of assets to a limited number of third parties - including their cyber

security providers. This would allow companies in their supply chain to better support and secure SoNS assets. This disclosure should be subject to applicable confidentiality requirements.

Recommendation: Amend the Bill to permit entities to disclose SoNS declarations of assets (subject to relevant confidentiality agreements etc.) to a limited number of third parties - including their cyber security providers.

Globally Accepted Standards to Underpin Incident Response Plans

Incident response plans are important to ensure that a SoNS entity has established processes and tools to prepare for, and respond to, a cyber indent. These plans can be important in assuring the Government and the community that Australia's SoNS entities are sufficiently prepared for cyber security incidents when they happen. The EM notes that SoNS entities' incident response plans would need to comply with any requirements specified in the rule, which may include details on procedures to be included in the plan for responding to a particular cyber security incident. We would encourage the Government to promote the use of globally accepted standards and best practices for incident response that are already widely adopted globally and across industries.[2] This will have the dual effect of encouraging the adoption of these best practices, while also avoiding the creation of possibly fragmented, duplicative, or conflicting requirements.

Recommendation: In developing rules and guidance materials on incident response plans, work with industry to draw on collective expertise and promote the use of globally accepted standards and best practices.

Welcome Collaboration on Critical Infrastructure Risk Management Program Rules

We welcome the proposed introduction of Risk Management Plans as a key pillar of the Government's critical infrastructure reforms. We believe the Risk management Plans have the ability to create real and meaningful cyber security uplift across the Australian economy and in turn foster a culture of cyber security. Palo Alto Networks welcomes the Government's engagement with industry in the development of the Risk Management Plans - Program Rules. These rules have been subject to revision via the industry consultation process and we believe the Program Rules are now amenable to both the public and private sector. We also welcome the alignment of the Risk Management Program rules and the Hosting Certification Framework under Subsection 30AB(5).

Conclusion and about Palo Alto Networks

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

[2] See NIST 800-61 Rev2, *Computer Security Incident Handling Guide* and the SANS Institute's *Incident Handler's Handbook*.

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: Contribution to Australia's Cyber Security Ecosystem

Palo Alto Networks is committed to helping Australian Governments at the Federal, State and Territory level embrace the digital world safely and protect their operations from cyberattacks. Palo Alto Networks undertakes a range of activities that contribute to strengthening Australia's cyber security posture, including actively supporting Governments at the operational and strategic 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 cyber security professionals. We provide Australian academic institutions with curriculum, technology, and faculty training at no cost via our Cybersecurity Academy Program. To date, we have 28 Authorised Cybersecurity Academy Centres in Australia. We are also a member of the Australian Government's Skill Finder Initiative - which provides free access to over 2000 online courses provided by the world's leading tech companies.

Finally, Palo Alto Networks undertakes activities across our community to raise cyber security awareness and engage the next generation on cyber security issues. With a mission to become the cyber security partner of choice, we launched our Cyber Safe Kids program in February 2020. This program aims to educate students aged 5-15 on the skills they need to protect their digital future and become good digital citizens. Palo Alto Networks stands ready to support Australian Governments to make each day safer and more secure than the one before. For more information see https://www.paloaltonetworks.com.au/