14 February 2025

Department of Home Affairs

Brindabella Park

Canberra, ACT, 2600

Submitted via CI.REFORMS@homeaffairs.gov.au

RE: Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)

Palo Alto Networks appreciates the opportunity to provide a submission in response to the Department of Home Affairs call for view on the Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).

Palo Alto Networks is the global cyber security leader, securing the networks, data and services of enterprise and Government customers 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 across governments and critical infrastructures.

We commend the Australian Government's leadership in cyber security and its commitment to delivering key initiatives under the 2023–30 Cyber Security Strategy. The progression of these legislative amendments is a significant step towards strengthening national resilience, enhancing cyber readiness and reinforcing Australia's ability to prevent, detect and respond to evolving threats.

Below, we provide feedback on two key areas of the Consultation on Subordinate Legislation—the draft rules relating to the Cyber Incident Review Board (CIRB) and the Ransomware Payment Reporting Regime. Our feedback focuses on the effectiveness, clarity, and potential impact of these measures, offering recommendations to strengthen their implementation and ensure they achieve their intended objectives.

In providing the feedback below, we draw on our extensive cyber incident response and threat intelligence capabilities, which regularly research and respond to cyber actors including nation-state actors and cybercriminal groups. Our team of over 250 threat researchers work across complex cyber threats, bringing deep insights into vulnerabilities, attack patterns, mitigation strategies, and evolving adversary tactics. Additionally, we leverage our extensive experience as a leading incident responder, responding to major cyber incidents across the globe in all industry verticals. As recognised by the Forrester Wave Cyber Security Incident

Response Services report, Palo Alto Networks (Unit 42) is among the top five incident response companies globally.[1]

Our Unit 42 Team also supports hundreds of managed services clients globally, delivering comprehensive managed detection, response, and threat hunting services that provide deep visibility into emerging threats and adversary behaviors. In addition, we offer premier consulting services to many of the world's largest organisations, including red/purple team exercises, attack surface assessments, and advanced attack simulations. These engagements not only enhance our clients' defensive capabilities but also provide critical insights into real-world attack methods and security gaps, helping organisations understand their exposure and improve their overall cyber resilience.

Our deep expertise, combined with our role as a founding industry member of the U.S. Cyber Safety Review Board, ensures that our insights are grounded in real-world threat intelligence, cutting-edge response strategies, and a global perspective on cyber resilience.

Draft Cyber Security (Cyber Incident Review Board) Rules 2024

We strongly support Australia's creation of a Cyber Incident Review Board (CIRB) and believe it will drive meaningful change and uplift the nation's cyber resilience. By fostering a culture of transparency and continuous learning, this initiative has the potential to improve incident response, share critical insights, and prevent repeat attacks. A strong emphasis on industry engagement will be key to securing support from the private sector, ensuring that lessons learned translate into tangible improvements across the economy.

A key strength of the Draft Cyber Security (Cyber Incident Review Board) Rules 2024 is the structured review process, which ensures a clear and systematic approach for the CIRB to assess referrals and determine whether to conduct a review. We also welcome the requirement for security clearances, as this is essential to ensuring that those involved in the review process have appropriate access to classified and sensitive information, reinforcing the credibility and effectiveness of the CIRB. Additionally, we welcome the inclusion of conflict of interest management measures, which require members to disclose any potential conflicts, reinforces transparency and upholds the integrity of the CIRB's operations. In addition we offer the following areas of consideration to enhance the effectiveness and credibility of the CIRB in Australia's cyber security landscape:

1. **Recommendation: Refine Eligibility Criteria for Standing Board Members**

We strongly recommend that the eligibility criteria for standing board members be narrowed and refined to ensure alignment with the core functions of the CIRB. As currently drafted, the requirements for standing board members and expert panel members are almost identical, despite the distinct nature of their roles. Standing board members should possess a higher degree of cyber security and incident response expertise, while the expert panel can include a broader range of professionals to provide complementary insights.

[1] https://www.paloaltonetworks.com/blog/2024/06/forrester-wave-for-cybersecurity-incident-response/

The core function of the CIRB is to provide specialised cyber security and incident response advice. To fulfill this mandate effectively, standing members should be required to have deep expertise in cyber security, technical incident response, and related disciplines. While broad expertise is valuable for the expert panel, the standing board should be composed of individuals with direct, hands-on experience in cyber threats, mitigation, and incident handling.

We also recommend that the Government remove unnecessary criteria, including:

- Rule 13 (b) (iv) (which allows appointment based on holding a relevant Commonwealth, State, or Territory government position) should be removed. Most senior government officials meeting this requirement would already qualify under legal, cyber security, or public administration experience. This broad inclusion risks diluting the board's cyber security expertise.
- Rule 13 (b) (vii) and (viii) (which allow eligibility based on critical infrastructure experience or an academic background) should also be removed from the standing board criteria. While these qualifications are relevant for expert panel members, they do not guarantee direct cyber or incident response expertise, which is essential for the standing board. Additionally, experience in a single critical infrastructure sector—such as finance or telecommuinications—does not necessarily ensure the cross-sector expertise needed to assess cyber incidents across multiple industries and verticals. Given the diverse and evolving nature of cyber threats, standing board members should possess broad, multi-sector experience in cyber security and incident response, ensuring a comprehensive and adaptable approach to reviews.

These amendments would strengthen and refine the criteria for standing board membership, ensuring a focused emphasis on core cyber security and incident response expertise. By prioritising individuals with demonstrated experience across multiple sectors and verticals, the CIRB will gain diverse, real-world insights essential for effectively assessing and responding to complex cyber incidents. Narrowing and sharpening these criteria will enhance the Board's ability to deliver credible, expert-driven oversight, reinforcing its role as a trusted authority in safeguarding Australia's cyber security landscape.

2. Recommendations: Enhance Public Transparency Measures

The draft CIRB Rules include provisions for publishing notifications when a review is initiated, which is a positive step toward public awareness and accountability. However, the draft Rules lack detail on what information will be shared with the public and stakeholders during and after the review process, which could limit transparency and industry confidence in the Board's work.

To enhance public trust and ensure meaningful engagement, the Rules should provide clearer guidance on the extent of information that will be disclosed at different stages of the review. Striking the right balance between transparency and security considerations would reinforce

confidence in the CIRB's processes, encourage greater industry and public engagement, and maximise the impact of its findings on national cyber security improvements.

3. **Recommendation: Establish Period Reviews to Ensure Timeliness of Matters Under Investigation**

The draft CIRB Rules state that the Board must not conduct a review if it would interfere with an ongoing investigation. While this safeguard is prudent, there is no structured timeframe or escalation mechanism to ensure that reviews proceed once investigations conclude. Without clear parameters, reviews could be indefinitely delayed, reducing their impact in driving timely, actionable improvements.

To strengthen the effectiveness and accountability of the review process, the Rules should establish indicative timeframes for key stages, such as how long the Board has to determine whether to initiate or terminate a review after receiving a referral while an investigation is pending. Additionally, there should be an expected timeframe for completing a review once an investigation concludes, ensuring that findings remain relevant and actionable.

Incorporating mechanisms for periodic progress updates—such as requiring the Board to periodically assess deferred reviews and determine when they can proceed—would further enhance transparency, accountability, and the overall effectiveness of the CIRB in improving Australia's cyber resilience.

4. **Recommendation: Clarify Engagement with Affected Entity(ies)**

The draft CIRB Rules do not clearly define how and when affected entities will be engaged during a review, which is essential for producing accurate, practical, and actionable recommendations. Organisations directly impacted by an incident can provide critical insights into root causes, response challenges, and systemic vulnerabilities that may not be apparent from an external assessment. Without structured engagement, findings may be misaligned with operational realities, making them difficult to implement, while also limiting industry buy-in and trust in the review process.

We understand that engagement with affected entities may be addressed in the terms of reference for each review, allowing for flexibility based on the nature of the incident. However, we recommend that common principles for engagement be incorporated into the Rules to provide a consistent baseline for transparency, industry participation, and information sharing. This could include specifying when and how the Board will consult affected entities, how confidentiality will be managed, and whether affected organisations will have an opportunity to review draft findings before recommendations are finalised. Embedding these principles in the Rules will enhance the credibility and impact of CIRB reviews, ensuring they reflect diverse perspectives and contribute meaningfully to national cyber security improvements.

5. **Recommendation: Strengthen Language on Expert Panel Engagement**

The current rules and explanatory memorandum do not explicitly require that an expert panelist be involved in every review, instead stating that the Board "may" establish an expert panel to assist in the process. Additionally, the Government fact sheet reinforces this discretionary approach, stating that the Board "may" appoint expert panel members as needed.

We strongly recommend strengthening this language to require expert panel involvement in every review. Expert panelists bring critical technical, operational, and strategic perspectives, ensuring that reviews are conducted with specialised cyber security expertise and real-world insight. Their consistent participation would enhance the credibility of the process, strengthen industry buy-in, and improve the quality of findings and recommendations. Replacing "may" with "must" would provide greater clarity, ensuring that every review benefits from expert knowledge and a diversity of perspectives, ultimately improving the effectiveness and impact of the Board's work. Should the Government choose not to guarantee the involvement of expert panel members in every review, we recommend establishing a transparent decision-making framework that articulates the circumstances under which their inclusion may not be appropriate.

6. **Recommendation: Remove Rule 17 - Other Paid Work**

The restriction under Rule 17, which prohibits a Board member from engaging in any paid work that, in the Minister's opinion, conflicts or could conflict with their duties, raises concerns about how it will be interpreted and applied in practice. While the intent to prevent conflicts of interest is understandable and important for maintaining the integrity of the Board, the broad and subjective nature of this clause could significantly inhibit cyber security industry participation in the standing membership of the Board.

The cyber security industry is predominantly composed of professionals actively engaged in paid work across both the private and public sectors, including incident response, cyber threat intelligence, security consulting, and governance roles. If interpreted too restrictively, this provision may disqualify highly qualified experts from serving on the Board, limiting the diversity of perspectives and real-world expertise available to CIRB.

We note that Rules 15 and 16 already establish clear conflict-of-interest disclosure requirements, ensuring transparency both before and during a Board member's tenure. These provisions allow conflicts to be managed rather than creating a blanket restriction, making Rule 17 unnecessarily restrictive. Given the high demand for cyber security expertise, the CIRB should aim to attract top talent, not inadvertently exclude them.

To balance integrity with expertise, we recommend removing or refining Rule 17 to rely on existing conflict disclosure mechanisms rather than imposing a broad restriction that may unnecessarily and arbitrarily prevent industry experts from serving on the Board.

Cyber Security (Ransomware Reporting) Rules

We support the Draft Cyber Security (Ransomware Reporting) Rules 2024, which mark a critical step forward in strengthening Australia's cyber resilience by mandating the reporting of ransomware payments. This framework enhances government visibility into ransomware threats, enabling a more coordinated and informed response to cyber extortion activities. While the draft Rules introduce important measures, we offer the following recommendations to further enhance their effectiveness, improve clarity, and ensure broader compliance across the business community.

1. **Recommendation: Clarify Third-Party Roles and Responsibilities**

The draft rules and supporting policy documents should provide clearer guidance on the roles and reporting obligations of third parties involved in ransomware incident response. Many organisations rely on external incident response firms, legal counsel, or insurers to negotiate with ransomware actors and facilitate payment decisions, yet the current rules do not explicitly define their responsibilities under the reporting framework.

We strongly encourage the Government to clarify in the explanatory memorandum that while third parties can report on behalf of their clients if directed to, they are not responsible for ransomware payment reporting, even in cases where they may have executed the payment on behalf of the affected entity. Without this clarity, ambiguity could lead to underreporting, delays, or duplicate submissions, as different parties may assume that another entity is responsible for compliance. Additionally, legal and contractual confidentiality agreements between organisations and their service providers may create uncertainty around reporting obligations, further complicating compliance.

To address this, the Rules should explicitly clarify how reporting obligations interact with contractual agreements, ensuring that responsibility remains with the affected entity while allowing authorised third parties to submit reports on their behalf if needed. Providing this clarity will reduce compliance confusion, streamline incident response processes, and strengthen Australia’s cyber resilience without placing unnecessary burdens on organisations or their service providers.

2. **Recommendation: Regularly Revisit the Reporting Thresholds to Improve Visibility and Account for High-Impact Sectors**

While we welcome the alignment of reporting thresholds with the Privacy Act, which helps reduce regulatory burden and maintain consistency across legislative frameworks, the current threshold—applying only to entities with an annual turnover exceeding $3 million—limits reporting obligations to just 6.56% of Australian businesses. Given that ransomware actors frequently target small to medium enterprises (SMEs) due to their limited cyber security resources and expertise, this raises concerns about whether the Government will achieve its stated objective of improving visibility into ransomware’s full impact across the economy.

Beyond economic thresholds, the framework also fails to account for the sensitivity of the data held or the critical nature of the operations impacted by a ransomware attack. Many

small but high-risk organisations, such as NGOs, specialised healthcare providers and tech start ups, may fall below the threshold yet store highly confidential citizen data or provide essential public services. A ransomware attack on these entities could have significant consequences, including compromised medical records, disruption to community services, or exposure of vulnerable individuals' data. However, under the current framework, these incidents may go unreported simply because the affected organisation does not meet the turnover requirement.

To strengthen its effectiveness, we recommend lowering the reporting threshold or, at a minimum, introducing a periodic review process to assess whether the current threshold remains appropriate or if a broader, whole-of-economy reporting obligation is necessary. We also recommend considering alternative reporting criteria for entities that handle highly sensitive information or provide essential public services, regardless of revenue. This approach would ensure the regime remains responsive to evolving threats and provides a more accurate national picture of ransomware activity.

3. **Recommendation: Strengthen Reference to Tracking Ransomware Payments**

The draft rules and explanatory memorandum should more explicitly recognise the importance of tracking ransomware payments ("following the money") as a core objective of the reporting regime. One of the most effective strategies in combating ransomware is disrupting the financial incentives that drive these attacks, and the reporting regime presents a critical opportunity to track the flow of funds and identify patterns in ransomware payment transactions. While the current framework focuses on understanding ransomware's impact on infrastructure, customers, and threat vectors, it does not clearly establish the role of financial intelligence and law enforcement in tracing payments, identifying criminal networks, and disrupting ransomware operations. To maximise the strategic value of mandatory reporting, we recommend explicitly referencing the use of reported payment data for financial tracking and enforcement actions (for example explicitly as a "permitted purpose"). Strengthening this focus would enable better collaboration between government, law enforcement, and financial crime agencies, enhancing Australia's ability to disrupt ransomware actors and their funding mechanisms.

4. **Recommendation: Ensure the Reporting Regime Drives Real-Time Cyber Threat Intelligence Sharing and Enablement**

To be truly effective, the ransomware payment reporting regime must demonstrably improve cyber security outcomes by ensuring that reported data is rapidly analysed, enriched, and disseminated to industry in near real-time. The success of this framework should be assessed by how well the Australian Government leverages reported cyber incidents to generate actionable intelligence that protects businesses and critical infrastructure from evolving threats—not simply by the volume of reports collected or its inclusion in annual ACSC threat reports or quarterly snapshots.

To achieve this, the reporting framework should standardise reporting formats and support automated, programmatic data sharing to allow rapid analysis and redistribution of insights to industry. This should include integration with the Australian Signals Directorate's Cyber Threat Intelligence Sharing (CTIS) platform, ensuring that organisations can receive timely intelligence on ransomware tactics, indicators of compromise (IOCs), and evolving attack methods without unnecessary reporting delays. Rather than simply serving as a compliance mechanism, ransomware payment reporting should be designed to provide real-time, actionable intelligence to frontline cyber defenders, helping them detect, prevent, and mitigate attacks before they escalate.

5. **Recommendation: Amend Guidance to reference Reporting via Phone**

The current fact sheet specifies that ransomware payments must be reported via the online portal, but this could present a practical challenge for organisations experiencing a cyber attack. If an entity has been impacted by a ransomware incident, its systems or internet access may be compromised, making it difficult or impossible to submit a report online. To ensure accessibility and compliance, the fact sheet should explicitly clarify that reports can also be made via phone to the Australian Cyber Security Centre, allowing organisations to fulfill their reporting obligations even in the event of a major disruption. This additional reporting channel would enhance resilience, ensure timely compliance, and remove unnecessary barriers for affected organisations.

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, New Zealand and Indonesia (sasloan@paloaltonetworks.com).

About Palo Alto Networks - Palo Alto Networks is the world's cyber security leader. We innovate to outpace cyberthreats, so organisations can embrace technology with confidence. We provide next-gen cyber security to thousands of customers globally, across all sectors. Our best-in-class cyber security platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cyber security partner of choice. For more information, visit www.paloaltonetworks.com. For more information about *Palo Alto Networks Contribution to Australia's Cyber Security Ecosystem* please see https://www.paloaltonetworks.com.au/ or Palo Alto Networks Contribution to Australia's Cyber Capability.