Cybersecurity Coalition

February 29, 2024

Submitted via homeaffairs.gov.au online submission form

Department of Home Affairs
Government of the Commonwealth of Australia

RE: Cyber Security Legislative Reforms: consultation on proposed new cyber security legislation

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the Australian Government's public consultation on proposed new cyber security legislation. The Coalition appreciates the Australian Government's openness in engaging industry on this important topic and looks forward to working with the Government to ensure best cybersecurity practices are implemented in Australia.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. The Coalition has worked with more than 20 governments around the world on the development of national cybersecurity policies, many of which were designed to address issues that are raised in the paper.

Part 1 – New cyber security legislation

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

The Cybersecurity Coalition supports the stated objective in the consultation paper of a secure-by-design standard for consumer grade IoT which would, "align with international standards, ensure consistency between jurisdictions and minimize regulatory burden on Australian businesses, while also meeting our national security objectives."

The Coalition recommends that complying with a mandatory cyber security standard should be conducted through self-attestation by product manufacturers. Self-attestation could then be subject to review or audit by a third-party administrator. Manufacturers that self-attest should file documentation that supports the attestation with a third-party administrator and be liable for fraudulent attestations.

2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?

Yes, the first three principles of the ETSI EN 303 645 should be used as a baseline. The standard represents a solid foundation for enhancing the security of consumer-grade IoT devices sold in Australia. These principles reflect widely recognized best practices in cybersecurity and underscore the importance of addressing common vulnerabilities that can compromise the integrity and safety of IoT ecosystems.

3. What alternative standard, if any, should the Government consider?

The Coalition supports the proposed approach outlined by the Department of Home Affairs in the consultation paper which would allow for replication of the flexible approach taken in the SOCI Act 2018 with relation to standards used by entities in preparation of their Risk Management Plans. This would allow for consistent approach across legislative regimes, which could be refined over time. For example, the United States Government through its Executive Order Executive Order on Improving the Nation's Cybersecurity, published in May 2021 has commenced work through the National Institute of Standards and Technology (NIST) within the Department of Commerce to develop standards aimed at ensuring consumers are able to make informed choices about buying IoT products. The Cybersecurity Coalition encourages the Australian Government to engage with NIST's ongoing efforts to define standards for IOT devices.

4. **Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?**

Determining the scope of smart devices subject to an Australian mandatory standard will require careful consideration of a range of factors. The Coalition encourages the Australian Government to conduct a further assessment of smart devices based on local needs, market dynamics, and engage further with stakeholders through consultation before defining the smart devices in legislation.

5. What types of smart devices should not be covered by a mandatory cyber security standard?

While the Coalition maintains the position that manufacturers, developers, and consumers should prioritize cybersecurity across all connected devices, there are certain categories of smart devices which do not warrant coverage under mandatory cybersecurity standard. In determining the types of smart devices that should not be covered by a mandatory cybersecurity standard the Coalition encourages the Australian Government considering a range of factors such as functionality, risk level, and impact on consumers. Examples might include extremely low risk devices with minimal connectivity or functionality that pose no risk – this could be standalone item like microwaves or legacy items no longer supported by manufacturers or lack firmware/software update mechanisms may present challenges in complying with cybersecurity standards but where other risk mitigations are present.

6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

The Coalition encourages the Australian Government to take a transparent and flexible approach to adoption of a new regime that is as broad and complex as this. Feedback on the UK's PSTI from stakeholders has been that there is a sense that there has been minimal publicity about the impact of the changes and concerns about the feasibility of bringing products into compliance in the timeframes allocated by the UK Government. Additionally, the inclusion of the new cybersecurity regime for consumer connectable products in legislation alongside telecommunications deployments may have also obscured the magnitude of the changes.

The Coalition encourages the Department of Home Affairs to work with stakeholders to provide a "roadmap for implementation" of any legislation developed, noting of course it would still first need to be passed by the Australian Parliament. This roadmap could outline steps to be taken by Government and those required of industry, such as engaging with a separate limited consultation process to aid in the definition of which products are subject to the standard. It would also allow the Australian Government an opportunity to engage with the UK Government and other stakeholders on lessons learnt from the implementation of the PSTI regulations and factor those into Australia's roadmap.

7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?

The Coalition encourages the Department of Home Affairs to take a similar approach to compliance and enforcement as it did with the SOCI act and abide by the regulatory principles and approach published by the Cyber and Infrastructure Security Centre, with a focus on taking a consultative approach with industry.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?

The Coalition supports an approach to mandatory reporting for ransomware incidents with the overarching aim of allowing for the provision of essential information by an entity to the Australian Government without overburdening the organization or hindering its ability to recover effectively. Striking the right balance between transparency and practicality is critical. While reporting can enhance our collective understanding of threats and responses, it must be implemented in a way that doesn't unduly burden organizations or compromise data security. To that end, three overarching mandatory fields of information could be sufficient for initial reporting:

- Incident Overview: affected entities should be able to provide a concise summary of the ransomware or cyber extortion incident, outlining when it occurred, how it was detected, and initial observations regarding its impact on the organization's operations. Additionally, information about vulnerabilities that were exploited and the tactics, techniques and procedures (TTPs) used by the attackers.

- Affected Assets: detail the systems, networks, or data sets affected by the incident.

- Initial Response: briefly describe the organization's immediate response actions, such as isolating affected systems, securing backup data, and activating incident response protocols to mitigate further damage. Additionally, consideration could be given to what communication, if any, has occurred with criminal actor perpetrating the attack.

9. What additional mandatory information should be reported if a payment is made?

Once again, the overriding objective should be to ensure organizations can recover as quickly as possible from any attack. As such the Coalition recommends the information should be limited to the amount and date of a ransom payment, and information about payment instructions (including any virtual wallet address).

10**. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?**

The Australia Government is in unique position to lead the world on a comprehensive policy approach to combatting ransomware to break the criminal business model that has developed. The Coalition encourages the Australian Government to consider developing a roadmap to banning ransomware. This could be outlined in the ransomware playbook being developed as part of the broader strategy. Increasing transparency around the issue through reporting is an important first step in the process.

We commend the Australian Government for pursuing the objective, as outlined on the new Strategy, of making it easier to meet regulatory obligations. To that end, the proposed ransomware reporting obligations should take into account other reporting regimes already in place, most notably the Data Breach Notification Scheme under the Privacy Act 1988. Wherever possible the goal should be for organizations impacted by a cyber incident to report once.

We encourage the Department of Home Affairs to collaborate with international partners to harmonize policy approaches in this endeavor. To that end, the Department should engage closely with the Cyber and Infrastructure Security Agency (CISA) as it will soon be publishing proposed rules implementing the ransomware reporting requirements within the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This act represents the most expansive cybersecurity regulations for the private sector in the US to date and will capture many organizations that will be subject to any Australian mandatory ransomware reporting requirements. Aligning reporting obligations with those in CIRCIA would significantly aide in entities fulfilling their Australian obligations.

11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

The Coalition suggests the Australian Government consider taking a phased approach to the implementation of the reporting obligation, by initially only introducing reporting upon payment of ransomware for entities with turnover of $25 million for the first year and subsequently requiring the two-stage reporting obligation outline in the consultation paper. The threshold for

reporting could subsequently be lowered to entities with turnover of $10 million as the regime matures and business have time to adapt to the requirement and have resources available, such as the ransomware playbook being developed as part of the 2023–2030 Australian Cyber Security Strategy

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

The Coalition suggest aligning the timeframe for reporting with the SOCI Act 2018 – so within 72 hours of payment. Additionally, the Australian Government should consider limiting the reporting requirement to payments made as the result of ransomware and not cyber extortion. This means that covered entities will not be required to report ransom payments made in response to other types of cyber extortion (for example, if an attacker downloaded data from an unsecured cloud account and demanded payment not to publish the data, such a payment would not be reportable). This would align with the CIRCIA Act.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

The Coalition assesses the assurance provided by no-fault and no-liability principles can significantly increase confidence among organizations when reporting ransomware or cyber extortion incidents. The most immediate benefit is the reduction of fear of legal or financial repercussions for reporting such incidents, thereby encouraging entities to come forward and disclose breaches. When entities are assured that they won't face blame or liability for reporting incidents, they can focus their efforts on mitigating the impact of the attack and preventing future occurrences.

14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

By adopting a holistic and collaborative approach to cybersecurity governance, beyond the reporting requirement. which is broadly seen in the initiatives outlined in the new Strategy, the Australian Government can encourage businesses to take responsibility for their cybersecurity while providing the necessary support and incentives to address the complex challenges posed by ransomware and other cyber threats. Along with establishing clear reporting guidelines the Australian Government can work to ensure encourage voluntary reporting by companies that fall outside the parameters of any new ransomware reporting legislation.

15. What is an appropriate enforcement mechanism for a ransomware reporting obligations?

Given the similarity that will likely exist between any ransomware reporting regime and that which already exists for critical infrastructure entities, consideration could be given as to whether the not the enforcement mechanism could be aligned with the SOCI Act 2018 enforcement mechanism. As per previous responses provide in this submission, the overarching regulatory principles and approach published by the Cyber and Infrastructure Security Centre, with a focus on taking a consultative approach with industry, should be adhered to.

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Given many ransomware incidents are perpetrated by ransomware threat actors using known vulnerabilities, the overarching goal of the reporting mechanism should be to use information garnered to notify other risk entities of vulnerabilities, so organizations can significantly reduce their likelihood of experiencing a ransomware event. Therefore, the Coalition encourages the Australian Government to consider moving to proactive model of ransomware information sharing, like that being trialed by CISA under its Ransomware Vulnerability Warning Pilot (RVWP). Under this pilot CISA proactively identifies information systems that contain security vulnerabilities commonly associated with ransomware attacks. After discovery, CISA notifies owners of the vulnerable systems. Notifications will often contain key information regarding the vulnerable system, such as the manufacturer and model of the device, the IP address in use, how CISA detected the vulnerability, and guidance on how the vulnerability should be mitigated.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National

Cyber Security Coordinator

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

The Coalition is supportive of the Australian Government's move to a limited use obligations for reports made to the Australian Cyber Security Centre. The purposes listed in the consultation are broadly appropriate however consideration should be given to specifying the use by Ministers of information obtained via reporting to ACSC and the Coordinator. Additionally careful consideration should be given to the definition of "stewardship" by regulators during an incident. Lastly, sharing of information directly with ASD as defined in the consultation paper to allow for the disruption or deterrence of threat actors raises questions of a vulnerability equities process and transparency of the use of a vulnerability garnered through reports made to the ACSC.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

When considering the restrictions that should apply to the use or sharing of cyber incident information several key tenets should guide ASD and the Coordinator. The use of cyber incident information should be strictly limited to specific purposes that serve the interests of national security, public safety, or the protection of critical infrastructure. These prescribed purposes should be clearly defined. Any use or sharing of cyber incident information must adhere to the Intelligence Services Act 2001 and the Privacy Act 1988 (where applicable). ASD should also maintain transparency regarding their use and handling of cyber incident information, including regular reporting on activities, oversight mechanisms, and mechanisms for redress in case of misuse or abuse.

19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

The Coalition is supportive of the new National Cyber Intel Partnership as practical mechanism to garner greater threat sharing prior to incidents occurring. It is a proactive initiative to increase resilience across the Australian economy. The Coalition recommends that this approach to proactive bi-directional information be fast tracked through the Strategies implementation. If organizations are able to see the value of information sharing this will encourage retrospective information sharing.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

The Coalition commends the Australian Government for pursuing the establishment of a Cyber Incident Response Board (CIRB). The listed functions and purpose outlined in the consultation paper are broadly acceptable. The primary recommendation the Coalition has is for the CIRB to be established as independent statutory agency akin to the Australian Transport Safety Bureau (ATSB); as maintaining independence when investigating incidents will be essential the CIRB's investigatory integrity.

21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?

To ensure that a CIRB does not interfere with the stated activities above, several limitations could be considered including clearly defining the scope and authority of the CIRB to focus solely on cybersecurity incidents and vulnerabilities within the private sector or critical infrastructure domains. However, the CIRB should be given scope to review the actions, processes and information sharing of Australia Government entities during a significant cyber incident and provide recommendations for areas of improvement. The Coalition recognizes that this could potentially create some friction as agencies could hypothetically invoke national security concerns to avoid scrutiny of their actions. Despite this, consideration should also be given to what powers the CIRB would be given to investigate incidents that also effect government entities and what protocols would need to be put in place to allow for this to occur.

Establishing clear protocols and mechanisms for information sharing between the CIRB and relevant government agencies will be crucial to CIRB's operations. Information shared with the board should be limited to non-sensitive, declassified, or anonymized data to prevent inadvertent disclosure of classified or sensitive information. The Coalition recommends establishing an independent oversight mechanism to monitor the activities and decisions of the CIRB, ensuring compliance with its established guidelines. It could potentially extend to reviewing board proceedings, accessing relevant documentation, and identifying potential conflicts of interest or undue influence. This oversight body would logically be the Parliamentary Joint Committee on Intelligence and Security.

22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

The coalition agrees with the articulation of the no fault principles in the consultation paper to align with those used by the ATSB.

23. What factors would make a cyber incident worth reviewing by a CIRB?

The Coalition supports the use of the broad definition used for instigation of an incident review used by the United States Cyber Safety Review Board which is derived from the Presidential Policy Directive (PPD) 41. The thresholds for instigation of an investigation should be publicly available and clearly outlined each time a review is commenced. Additionally, consideration should be given to how best to coordinate with international partners, particularly the US CSRB, on the commencement of an investigation given the borderless nature of large-scale cyber incidents. Developing a MOU with the US CSRB would be beneficial in this regard.

24. Who should be a member of a CIRB? How should these members be appointed?

The Coalition recommends that the Australian Government consider appointing independent commissioners to the CIRB who will be responsible for executive oversight of the CIRB and functionally would conduct the bulk of any investigation and be responsible for signing off on reports issued by the board.

The Commissioners could be supported by an advisory board of Australian Government officials and industry and non-profit stakeholders to allow for expert insights be provided on any given incident. For example, the advisory board members could be drawn from organizations represented on the new Executive Cyber Council.

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

By virtue of the all-encompassing nature of digital risks and the likely reviews cutting across different technologies and industries, a multi-disciplinary membership will be needed.

Core domain expertise could include:

1. **Technical Expertise**: an understanding of technical aspects of cybersecurity, including network security, encryption, malware analysis, forensics, penetration testing, and secure coding practices.

2. **Incident Response Experience**: experience in incident response and crisis management bring valuable insights into effective incident handling procedures, incident triage, containment strategies, and post-incident analysis.

3. **Risk Management Knowledge**: Expertise in risk management principles and practices is essential for assessing the potential impact and likelihood of cyber threats, prioritizing response efforts, and developing risk mitigation strategies.

4. **Legal and Regulatory Compliance**: expertise in cybersecurity laws, regulations, and compliance frameworks can provide guidance on legal and regulatory obligations related to incident reporting, data protection, privacy rights, and breach notification requirements.

5. **Industry-Specific Knowledge**: Domain-specific expertise in industries such as finance, healthcare, energy, government, and critical infrastructure sectors is valuable for understanding sector-specific cyber threats, regulatory landscapes, operational challenges, and best practices. Drawing upon expertise that already exists in the Trusted Industry Sharing Network (TISN) could be one way to harness industry-specific expertise depending on the type of incident.

6. **Policy and Governance Experience**: Members with experience in cybersecurity policy development, governance frameworks, international affairs, national security policy and organizational leadership.

7. **Cyber Threat Intelligence**: Expertise in cyber threat intelligence analysis, threat hunting, and information sharing practices enables CIRB members to identify emerging threats, adversary tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs). Threat intelligence specialists can inform incident reviews with actionable insights and proactive threat mitigation strategies.

Above all, members will need to have excellent communication and collaboration skills to engage with stakeholders, articulate findings and recommendations, facilitate cross-functional teamwork, and foster a culture of transparency.

26. How should the Government manage issues of personnel security and conflicts of interest?

Ensuring the integrity and impartiality of the CIRB will be critical to its success. The Coalition recommends that the Department of Home Affairs develops a system to identify, mitigate, and manage any conflicts of interest that may as a result of an individual's participation in the work of the CRIB. Ideally this system and its precepts would be made public.

27. Who should chair a CIRB?

In line with the response question 24, the Coalition supports the idea of an independent commissioner/chair of the board, appointed by the Australia Government, in line with the governance structure of the ATSB.

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

As per the response to question 23, the process and decision making for instigation of an investigation should be made public. Ideally an elected official of parliament would have final sign off on commencement of an investigation, based on advice from the National Cyber Security Coordinator. Importantly, the Department should consider a process for consultation with industry on the merits of instigating any investigation as it is likely the incident would already be public in nature and insights from beyond government will be important for the framing and scope of an investigation.

29. What powers should a CIRB be given to effectively perform its functions?

CIRB should be endowed with powers to effectively perform its functions without the Australian Government providing it with subpoena powers, which could undermine trust in the institution and be seen as overly intrusive and burdensome by some entities. Without subpoena power, the focus remains on voluntary cooperation, information sharing, and collaborative problem-solving to address cybersecurity challenges effectively.

30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

Ideally information provided to the CIRB would be covered under any limited use obligations regime created for the ACSC and the Cyber Coordinator.

31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

Initially, limited enforcement mechanisms should be put in place for the CIRB. The CIRB should seek voluntary information provision to foster a culture of cooperation and collaboration among stakeholders, including private sector entities, government agencies, industry associations, and cybersecurity experts. Encouraging voluntary participation and information sharing will allow for the CIRB to be seen as an impartial mechanism for open dialogue and knowledge exchange.

The CIRB should factually, and with appropriate context, publicly acknowledge in its reports where an organization has declined to provide information. Once the CIRB is established and a review of its information gathering powers could be conducted to ascertain if subpoena powers and enforcement mechanisms are needed.

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

As per previous responses, a governance structure which allows for creation of the CIRB as a statutory body outside any existing government department, with independent commissioners/chairs overseeing its management will set it up from the outset as a credible and impartial body. Regular mandated reviews of the operations of the CIRB will also assist in maintaining its credibility, along with engaging with international partners to exchange best practice.

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

The Coalition acknowledges that the CIRB will likely be accessing and reviewing sensitive information but strongly encourages the Australian Government to allow for as much transparency as possible with relation to the board's findings. As seen with CISA's Shields Up campaign in the run-up to Russia's invasion of Ukraine, national governments can walk the line between national security equities while also ensuring that the information is getting to organizations that can reduce cyber risk across the economy. For this reason, the Coalition encourages the Australian Government to avoid using redaction wherever possible, with obvious exceptions where information directly identifies individuals.

Respectfully Submitted,
The Cybersecurity Coalition

February 29, 2024

CC: Ari Schwartz, Venable LLP
Adam Dobell, Venable LLP