Cybersecurity Coalition

February 1, 2022

Submitted via homeaffairs.gov.au online submission form

Department of Home Affairs
Government of the Commonwealth of Australia
3 Lonsdale St,
Braddon ACT 2612, Australia

RE: Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the public consultation issued by the Australian Government's Department of Home Affairs ("the Government") on its *Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* ("the Draft Bill"). The Coalition appreciates the opportunity to comment on the Draft Bill and looks forward to working with the Government to further explore the adoption of proposals outlined in the paper.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

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 Draft Bill. We are acutely aware of both the need to effectively manage threats to critical infrastructure, as well as the difficulty of doing so in an effective manner, given the complexity of cybersecurity.

The Coalition strongly supports many of the Draft Bill's provisions. These include:

- The decision to develop Risk Management Programs ("RMP") on a sector-by-sector basis, enabling greater specificity in how risk management measures are tailored to the each sector's needs;
- The 'on switch' approach to RMP, which helps to avoid unnecessary changes where sufficient industry standards and best practices are already in place;

- The use of a 'public interest criteria' and public consultations before determining whether an existing sectoral framework needs to be replaced or updated, to enable for a fair and transparent assessment of the need for such measures;
- Efforts to deconflict requirements where entities have assets that cut across regulatory jurisdictions, which could otherwise place companies between conflicting requirements;
- The emphasis on bi-directional information sharing, which will better enable critical infrastructure to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events;
- Ensuring that annual reporting requirements are not overly onerous in terms of the information required, which would focus resources away from operational activities; and
- The determination of Enhanced Cyber Security Obligations ("ECSO") on an entity-by-entity basis, with no automatic obligation and a stated preference by the Government towards voluntary cooperation, as this more efficiently leverages industry capabilities and builds greater industry-government trust.

Nevertheless, we believe the Draft Bill could be adapted to better achieve the Government and industry's shared objective of ensuring that Australian Critical Infrastructure is sufficiently resilient in the face of rising cybersecurity threats. Specifically, we recommend that the Government:

<u>RMP</u>

1. Establish a clear *mechanism* for owners of assets that are covered by more than one sector to appeal against the adoption of RMP provisions that will force them to contravene the requirements of another sector. This will give a clear channel for industry and government to address such concerns and promote consistency across sectors.

2. Take a more outcome-focused approach to critical infrastructure risk management. Rather than mandating that covered entities take specific steps or individual mitigation measures, regulators should clearly articulate their desired outcome and enable the asset owner to determine the most effective way to meet that standard.

<u>Thresholds for CI</u>

3. Narrow the proposed scope of 'data storage and processing service' and 'data storage and processing asset' to ensure that those entities with low systemic risk are not unnecessarily subject to these requirements. This can be achieved by retaining "wholly or primarily" in the definition of 'data storage or processing service' and 'data storage and processing asset', rather than remove it, as is currently proposed.

Systems of National Significance ("SNS") and ECSO

4. Provide greater clarity as to whether the private nature of SNS designation and ECSO prohibits company officers from notifying owners, shareholders or other interested parties. If so, the Government should provide company officers with a clear exemption from any obligations under Australian law to notify shareholders of material information (for example if they are directed by ASD to install unknown software on their systems). They should also provide guidance as to how officers should approach such requirements where they exist in other jurisdictions to which they're subject.

5. Provide greater clarity regarding the kind of threat intelligence that the Government intends to provide to industry and who will be eligible to receive it. Timely, accurate threat intelligence is a valuable tool to companies of all sizes and levels of criticality. Facilitating the cybersecurity industry's receipt of this information, for example, would greatly enhance the distribution of such information to critical and non-critical infrastructure clients with whom they work.

6. Provide greater clarity as to what circumstances would lead to the requirement to provide minute-by-minute system information reports, as well as the timeline for implementation (making such automated threat information available to the government).

7. Remove requirements to conduct cybersecurity exercises on a topic of the governments choosing and replace them with a process for the Government to disseminate recommended topics for exercises. While cybersecurity exercises can be an invaluable tool in developing and testing cyber risk management programs, their utility stems from their relevance to an organization and buy-in from operational leaders. An imposed process such as this will serve as a check-the-box exercise and may have little improvement to security outcomes if not aligned with a company's risk management program.

8. Remove the ability for the Government to compel an SNS to install third-party software of the Government's choosing. Such powers not only represent a significant overreach in terms of the precedent that it sets, if the SNS does not have sufficient understanding or familiarity with the software, the installation and usage of such software could have a negative impact on the continuity of the digital systems.

9. Implement a mechanism for oversight of how these powers are used. Ideally this would include some level of public transparency, as well as a mechanism for appealing an SNS designation. Such measures ensure that such extraordinary powers are utilized in a manner which befits Australia's democratic institutions and strong commitment to the rule of law.

The Coalition thanks the Government for its careful examination of complex issues. As the conversation around cybersecurity in Australia continues to evolve, we welcome the

opportunity to further serve as a resource on both technical and policy questions to ensure that these proposals are successful in achieving the Government's objectives.

Respectfully Submitted,
The Cybersecurity Coalition

February 1, 2022

CC: Ari Schwartz, Venable LLP
Alexander Botting, Venable LLP