Cybersecurity Coalition

February 10, 2021

Submitted via Parliament of Australia website

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Re: Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the public consultation issued by the Parliament of Australia ("Parliament") regarding the *Security Legislation Amendment Critical Infrastructure Bill 2020* ("the Bill"). The Coalition appreciates the opportunity to comment on the Bill and looks forward to working with Parliament to establish a robust approach to protecting Critical Infrastructure and Systems of National Significance.

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. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

As leaders in the cybersecurity industry, we recognize the complexity and importance of securing critical infrastructure. As written, the Bill would lead to improvements in Australia's cybersecurity posture. Nevertheless, there are important ways in which we believe the Bill could be further strengthened, to better achieve the Government's stated objective of uplifting the security and resilience of Australia's critical infrastructure. We have provided detailed comments regarding how to do so in the following section.

The Coalition thanks Parliament for its careful examination of complex issues. We also commends Parliament for making this Bill available for public comment, as suggested in our comments on the proposed Exposure Draft in November 2020.

Cybersecurity Coalition

As the conversation around critical infrastructure security in Australia continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that the Bill is successful in achieving the Australian Government's policy objectives.

Respectfully Submitted,
The Cybersecurity Coalition

CC: [redacted]

Cybersecurity Coalition

Detailed Comments

Stakeholder Engagement

Given the inherent importance of public-private partnerships to critical infrastructure security, we welcome the Government and Parliament's ongoing commitment to stakeholder engagement, including:

- Launching public consultations in preparation of the Critical Infrastructure Bill currently before Parliament;
- Article 18AA(2)(a)(ii) of the Bill, which requires the Minister solicit stakeholder input on any future amendments; and
- Commitments in Section 5.3 of the Explanatory Document to engage in a co-design process with critical infrastructure entities on a sector-by-sector basis, to determine sector-specific security requirements.

The Bill, sectoral regulations, and implementation will no doubt be more impactful for the input provided during these consultations.

Given the complexity of these issues, however, we would encourage the government to expand the proposed public consultation period in Article 18AA(2)(a)(ii) from 28 to 60 days. This will enable stakeholders to fully assess the implications of proposed regulatory changes and provide more helpful input to the Government. It would also bring Australia in line with the draft OECD Best Practice Principles on Stakeholder Engagement in Regulatory Policy, of which the Australian Government is a member, which recommends up to a 60-day comment period.[1]

The Coalition would also welcome clarification as to which stakeholders will be able to participate in the co-design process. The Explanatory Document references the participation of "key industry stakeholders," which is rather ambiguous. Where possible, we would encourage the incorporation of both critical infrastructure entities and cybersecurity service providers into those discussions, to ensure that the Government can ascertain the impact of a proposed approach on both a sectoral and national level.

[1] http://www.oecd.org/gov/regulatory-policy/BPPs-for-Public-Consultation.docx#:~:text=The%20aim%20of%20the%20Principles,on%20Regulatory%20and%20Policy%20Governance.

Cybersecurity Coalition

Implementation Period

Section 7.3 of the Explanatory Document states that the Positive Security Obligations "will not be applied to critical infrastructure assets until the sector-specific co-design has been completed and the sector-specific rules have been made. There will be a six month 'grace period' following the introduction of the sector specific rules."

While many critical infrastructure entities will find themselves largely in compliance with their sectoral PSOs already, this is a short transition time for those that are not. To seamlessly transition one's approach to security risk management is a complex endeavor, particularly given the potential for divergent requirements internationally. A shortened timeline for doing so further increases the challenge of doing so in a seamless manner.

Given the potential scope and penalties outlined in the Bill and the complexity of transitioning one's security practices, we encourage Parliament to make the timeline for transition "as soon as is practically possible and not more than twelve months following the introduction of the sector specific rules."

Sectors and Thresholds

The classification of Data Storage or Processing as a critical infrastructure sector is not aligned with international approaches, such as those taken in Europe or Japan. This sector would be better classified as a sub-section of Communications & IT critical infrastructure to ensure consistency and avoid misinterpretation of the intended scope of the Bill.

The thresholds for inclusion as a critical infrastructure entity within this sector (as defined in 12F) and many other sectors appear to be significantly lower than in other developed countries. With more than five hundred organizations expected to be captured within the healthcare, education and data storage sectors alone, it's likely that the number of critical infrastructure entities will exceed 1,000 in total – far more than the equivalent designations in the U.S. or U.K., both of which have larger economies and populations.

By capturing too many organizations within the critical infrastructure designation, Parliament risks diluting the resources that it provides to the most critical entities, as resources provided to the 178th most critical higher education institution can no longer be directed to the most critical. In order to ensure that Government resources are dedicated to managing the most significant risks to Australia's digital infrastructure, we strongly urge the government not to designate critical infrastructure in an unnecessarily broad manner.

Finally, the Bill should provide clear guidance that critical infrastructure entities will not be required to report to more than one regulator, which would introduce unnecessary complexity

into the cybersecurity activities of critical infrastructure entities, while wasting government resources. Regardless of which regulators are chosen, it's important that they maintain close working relationships with the ACSC and Australian Signal Directorate - given their cybersecurity expertise.

Security Measures

We are glad to see that the Bill balances the need for sector-specific security requirements to address the different risk profiles of different industries, while also providing a series of overarching outcome-focused principles for regulators to follow. The Government's ability to appropriately balance the specificity and consistency needed will be key to the effectiveness of the proposed approach.

By clearly communicating desired outcomes and maintaining an open dialogue with critical infrastructure entities, while affording them flexibility in how the meet those outcomes, entities can best tailor risk management activities to meet specific needs. Regulators' can help companies to understand what is expected of them by providing guidance that:

- Clearly identifies what outcomes they want entities to meet.
- Demonstrates how companies will be assessed against those outcomes or are able to demonstrate compliance with them.
- Provides examples or references to best practices (e.g. consensus-based international standards).

The Government should, however, take responsibility for driving consistency across sectors and with other countries in terms of security requirements. Guidance should be provided to regulators regarding how they can best meet their responsibilities in this regard – in particular through the use of consensus-based international standards – to ensure that they do not introduce unnecessary complexity into the risk mitigation activities of critical infrastructure entities.

Moreover, the government should ensure that critical infrastructure entities whose business spans multiple sectors are not forced to report to multiple regulatory entities or comply with divergent security requirements.

Wherever possible, security requirements should be grounded in consensus-based international standards[2] to ensure alignment with international best practices and avoid

[2] Examples of such consensus-based international standards include: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1; ISO/IEC 27100, 27103 & 27110; ISO/IEC 27001; ISA/IEC 62443; COBIT 5; CIS Critical Security Controls; and NIST 800-53.

introducing unnecessary challenges or complexity into cybersecurity activities. In addition to the security benefits of interoperability, such an approach will also to avoid the establishment of unnecessary barriers to trade, which may have an adverse effect on Australia's economy. We are glad to see pp.284-285 of the Explanatory Document reference stakeholder feedback regarding the need to utilize international standards and hope that such an approach will be taken when implementing the Bill.

Threat Information Sharing

We are delighted to see that the Bill promotes an expanded threat intelligence sharing architecture to provide critical infrastructure with a more holistic picture of the threat landscape. This is particularly relevant given the cross-border, cross-sector nature of many significant cybersecurity incidents.

In order to achieve this objective, we encourage Parliament to place a stronger emphasis on the declassification of threat information, where possible, to better facilitate the real-time sharing of information with industry. This would be invaluable in providing industry with timely and relevant information through which to detect and mitigate threats.

To more effectively collaborate on an operational level to address real-world cybersecurity challenges, Parliament should establish a program in which private-sector experts can work alongside ACSC experts at a declassified level on a part-time basis. The United Kingdom's Industry 100 program provides an example of how this can be implemented in practice.

In terms of the sharing of information by industry, there are three principles that the Bill should adopt. Firstly, whenever critical infrastructure entities share information voluntarily with Government, they should have a clear understanding from the outset of how that information will be used and with whom it may be shared. Use of Traffic Light Protocol is one means to achieve this. The Bill should provide assurances that under no circumstances will they be able to share information beyond the terms agreed without the explicit consent of the original source of information. Such an approach is an effective means to build trust across the critical infrastructure community.

Secondly, under no circumstances should the Bill mandate timelines for critical infrastructure to share threat information. Mandates to share information by one government encourages other government to implement similar measures as each seeks 'first access' to indicators of compromise. Ultimately, this will lead to the mandatory sharing of information with untrusted entities.

Cybersecurity Coalition

Thirdly, the Bill should provide assurances that information shared by critical infrastructure for the purposes of security risk management will be shielded from Freedom of Information-type requests. Failure to do so will provide a chilling effect on information sharing as companies risk sensitive security information making its way into the public domain.

Finally, for companies that share cyber threat information, the Bill should provide limitations on liability, antitrust enforcement, and on regulatory disclosures. It is critical for these protections be in place to ensure threat informant can be shared without fear of negative consequences as these protections will maximize threat sharing.

Incident Reporting

The Coalition has two specific concerns with the proposed incident reporting requirements included in the Bill. The first of these pertains to the threshold for reporting incidents outlined in sections 30BD(1)(b)(i) and 30BD(1)(b)(ii). Our interpretation of "attempted access to a network where the entity believes a compromise is imminent" and "…or is likely to have a relevant impact on the asset" is that it would require companies to report not only incidents but attempted incidents.

If so, this is an incredibly broad interpretation that may result in companies have to report hundreds of thousands of incidents per day. In doing so, it would create a signal-to-noise ratio that would overwhelm governments and undermine their ability to provide timely, actionable intelligence to critical infrastructure. We request that the Bill clarify that attempted incidents are not *required* to be reported, though companies may wish to where it provides actionable intelligence.

In addition, the timelines for reporting outlined in 30BC and 30BD, 12-hours and 72-hours respectively, are unnecessarily short. Beyond the operational challenge that injects into the already challenging process of incident response, it greatly increases the likelihood that inaccurate or inadequately contextualized information will be shared with government by industry. We strongly recommend that the Bill replace arbitrary timelines with a requirement for companies to report within an appropriate timeframe.

Avoid Unnecessary Administrative Burden

It is critical that the desire to implement measurable security obligations not inadvertently become an exercise in check-the-box compliance, subordinating the iterative nature of risk mitigation to a rigid process of legal compliance. The Government should encourage regulators

to avoid imposing an overly prescriptive approach to security, which emphasizes static compliance over ongoing cyber risk management best practices.

This is particularly relevant to the proposed Board-approved annual reports for all critical entities, as well as the period and events-based reports for Systems of National Significance. While we understand the desire to foster awareness of cybersecurity among senior officials in critical infrastructure entities, such a process is unlikely to achieve this objective. It will, however, impose a notable administrative burden on critical infrastructure companies.

Moreover, we are concerned that these reports are likely to be a treasure trove of information for malicious cyber actors, as well as containing highly sensitive commercial information. Collating such information for potentially hundreds of companies, to be retained by multiple government agencies risks creates a potential vulnerability which may well outweigh the benefits of the proposed approach.

Depending upon their content and intent, the proposed playbooks and exercises for ECSO's can be a useful in improving incident response. They often have significant limitations, however, in terms of their utility, given the need to incorporate a wide range of (often unknowable) factors that may define a given incident, while requiring a significant investment of resources to develop and maintain. Moreover, the playbook itself can become a vulnerability – providing important information to would-be attackers.

Accordingly, we believe that the Bill and its implementation should provide flexibility in terms of whether and how they require companies to utilize these mechanisms. In particular, where a company can demonstrate its existing compliance with the regulatory objective, they should be exempted from duplicative activities. In other cases, the Government should carefully consider the relative merits and specific circumstances under which playbooks deliver a superior return on investment to critical infrastructure from a security perspective.

Government Assistance

The Government should apply a high threshold for when it can take direct action, with a strong preference in favor of directions to the entities being targeted in the first instance. To maintain public confidence, the execution of the power should be rare, reasonable and proportionate. It is also critical that a process be established for robust oversight of these powers. This should include both legal experts, who can determine the legality of decisions made, and technical experts, who can determine the need and proportionality of directives or direct government action. We believe that the Bill takes some steps towards achieving these objectives.

An approach that requires sign-off from multiple government officials is particularly relevant to the cyber context, as operations and policy currently sit across the two portfolios. It is reasonable to expect that in making a decision on 'direct action' that the Minister of Defence and Secretary of Home Affairs are in agreement on the merits of direct action and its necessity. We would encourage Parliament to go further and require the sign-off of the Attorney General in order to authorize such powers.

All direct action should be tightly defined and controlled - articulating what the Government and its officials can do, for how long and why. This should also specify that Commonwealth officers cannot conduct offensive cyber activities from within private sector infrastructure. Moreover, where possible, oversight of these new arrangements should be at a declassified level to maintain transparency of government, build public trust and confidence.

Finally, given the extraordinary nature of the proposed powers, there should be strict penalties for officials that attempt to utilize these powers without appropriate authorization, or in a manner that exceeds the authorization granted.

While companies may in many cases welcome government support in response to an imminent or ongoing major security incident, it's critical that entities have the ability to appeal a directive or direct government intervention to an independent arbiter, should they believe that the action is unnecessary, unfeasible or counter-productive in terms meeting the Government's stated security objectives.

While we understand the need for speed and flexibility in responding to such threats, we believe that the process would greatly benefit from the ability of critical infrastructure to avail itself of an appeals process to avert the potential impact of a misdirected directive. Even in the domain of national security, some level of judicial recourse is critical to underpinning the rule of law.

Liability from civil and criminal action against both companies and individuals, where their activities adhere to the intent of a government directive is both fair and critical to driving adherence. Failure to provide such protections will place critical infrastructure entities and their employees in the unacceptable position of being liable to criminal or civil action whether they comply or not. This would potentially create a chilling effect on the relationship between the government and private sector and may undermine the ability of companies to hire qualified employees for certain cybersecurity roles.

Moreover, it's important that the Government clarify whether immunities are afforded to subcontractors of critical infrastructure entities. For example, whether immunities would apply to a cybersecurity company that takes actions on behalf of their client at the direction of the Government. It should also address liabilities and immunities in the event that a government

directed change adversely impacts other customers or causes the entity or their vendors financial losses.

Depending upon the nature of the directives or direct action taken by government, the potential risks and costs to critical infrastructure entities are multifold. These include:

- Potential civil or criminal legal action against the entity or its employees
- Damage to equipment or infrastructure
- Loss of revenue from disruption to service
- Reputational damage

Where other governments, such as the Government of Thailand, have proposed adopting similar powers, they have typically addressed these concerns by establishing a mechanism for reimbursing private entities for damages caused in the process of executing a directive or in which the government takes emergency actions on their networks.

Beyond the financial relief that this affords companies – reducing the risks associated with compliance – it also ensures that the Government is not blind to the material costs of compliance, encouraging them to balance those against the potential costs of a major security incident. We urge Parliament to incorporate such provisions into the Bill.