27 November 2020

Submission on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

As a member of the Industry Advisory Committee to help guide the implementation of Australia's Cyber Security Strategy 2020 and one of Australia's leading professional services firms with an extensive network of strong relationships across the critical infrastructure sector we are well placed to share our perspectives on these important issues. Our engagement with and contributions to the sector in establishing the Australian Energy Sector Cyber Security Framework (AESCSF) with AEMO and our work with Home Affairs and the ACSC show we are committed to contributing to the Australian community and supporting and enabling initiatives that will strengthen the future prosperity of our country.

PwC welcomes the release of the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Draft Bill) and believes it is an important initiative in securing Australian critical infrastructure and supporting national resilience.

Overall, the Draft Bill appears in line with the three initiatives set out in the Consultation Paper. We consider the Bill in the context of the broader Government direction - specifically that this Bill is to be a foundation for a broader legislative framework which will apply to various sectors and will reflect the uniqueness of each sector. Sector regulation will involve further and more specific consultation which should capture more detail that cannot be reflected at this broad level.

Two important factors in the economy wide reform are the pace of implementation and its scope. We understand and fully support the Government's need to continue to move at pace to implement these reforms. We believe that improving clarity would enable the sector to maintain the pace of introduction while also ensuring the quality of implementation remains high. With this in mind, we believe there are some opportunities for improvements that would greatly assist with the smooth and timely implementation of the Act, particularly for owners and operators of critical infrastructure. Our detailed feedback is below. We would welcome the opportunity to discuss our views further. Please contact us using the details below.

Kind regards

[redacted]

[redacted]

Corinne Best
Partner, Trust and Risk Business Leader
PwC Australia
Direct: [redacted]
Email: [redacted]

Robert Di Pietro
Partner, Cyber Security
PwC Australia
Direct: +[redacted]
Email: [redacted]

Detailed feedback

Key PwC recommendations:

1. **Clarify what success in meeting obligations looks like so that industry have something to aim for and ensure speed and quality of implementation**
2. **Provide more specific detail around expected outcomes and scope of obligations.**
3. **Provide greater clarity on how companies private data will be used, stored and secured by the Government agencies receiving it**
4. **Describe the scope for a reportable incident for a provider of critical infrastructure to ensure it serves its purpose**
5. **State more specifically what will be classified as 'Critical Infrastructure' to give clarity to industry and assist with planning**

Broad Observations on Enhanced Cyber Security Obligations

The Exposure Bill is deliberately non-prescriptive in setting out how organisations should adhere to these new obligations. Although this is an approach that reflects the varying levels of maturity and initiative and therefore allows flexibility for organisations to choose their own path to meet expectations it introduces ambiguity as to whether expectations have been met. We suggest industry and Government should work together to close the gap in terms of the specifics of what is required and what 'good' looks like. We believe there is an opportunity to provide more detail about the requirements and how they should be achieved as they relate to the four following areas.

1. Cyber Security Exercises and Vulnerability Assessments: Division four of the Draft Bill sets out the requirements for Cyber Security Exercises and Vulnerability Assessments. In considering what an 'exercise' might mean for various entities there is a broad spectrum of effort and intensity from table-top exercises, to fully functional simulation and system testing. Similarly, vulnerability assessments can be simple automated scans (common for IT networks), or more complicated walkthroughs with physical inspection (for OT environments, where scanning is often not possible). Greater granularity is required to reassure entities as to what is expected, and this guidance could be applied based on organisation type, criticality, or nature of technology (IT, OT). If Government does not wish to be prescriptive in these areas and intends to let CI operators decide the best approach for themselves, we suggest more detail should be provided around the outcomes, objectives and 'measures of success' for these exercises and assessments.

2. Telemetry: Similarly for Telemetry (referenced in the Draft Bill in Division five), the extent and duration of the telemetry requirement could be made clearer and the process for how the Government will ensure the security of the data conveyed will be critical to building confidence with industry for this engagement. Speaking in detail about how the data will be managed will be important for both domestic and multinational entities who need to satisfy boards, customers and shareholders about data management and may also be required to satisfy local legislation about data.

The Bill should also seek to align with the work of the Office of the National Data Commissioner and especially the proposed *Data Availability and Transparency Bill 2020* which was released for public comment in September 2020.

3. Notifications: We believe the process or standard for what constitutes an event/incident that requires a notification (outlined in Part 2B of the Draft Bill) could be more clearly explained. Using an extant classification such as the Australian Cyber Security Centre Incident Categorisation Matrix may be a good initial step to overcome the challenge of entities classifying events/incidents differently. Important to this consideration is the fact that what might be an incident/event for the purposes of national security may not have the same effect/impact as an incident/event that affects system performance - as such, the ACSC classification scheme may not reflect the depth or subtlety required to manage incident detection for the purposes of national defence. In this regard, if there is a need to classify incidents that may not directly confer a threat to the entity, consideration will need to be given on how this classification standard detail and share accountability could be achieved for notifications across the sector.

4. Nominations and Directives: the internal government machinery that will support nominations of a CI system or SON is somewhat ambiguous. This is not directly relevant to entities and operators as it pertains to how the Government will internally manage the administration of enforcing the Act. However greater transparency around how this is achieved builds the dialogue with industry and fosters a productive working relationship. Industry will be seeking clarity on this issue and trying to understand what may cause them to be nominated and greater inclusivity and collaboration will support a productive engagement with industry. As per our previously presented views, there is an opportunity to establish a cross-sector criticality assessment framework that derives CI entities criticalities in a consistent standardised approach. A working example of this is the Criticality Assessment Framework (CAT) developed as part of the AESCSF. There is an opportunity here for Government and Industry to co-design a criticality framework.

Other comments on the Draft Bill and its implementation

Impact on Sectors

While the enhanced framework outlines a need for an uplift in security and resilience in all critical infrastructure sectors and the impact on industry is likely to be significant, we believe that the obligations as set out in the Draft Bill are achievable with sufficient guidance and support.

We would hope that - to reduce unnecessary burden - current Australian Government standards would be applied so as not to duplicate reporting or accreditation standards. Ideally, requirements/standards for various documentation and compliance reporting should align with the Information Security Manual, the Cloud Assessment and Authorisation Framework, the Notifiable Data Breach Scheme and the Protective Security Policy Framework.

The Exposure Draft shows due consideration for smaller companies and has identified means for government provided assistance, free or inexpensive software for those who may need it and additional support and advice for companies. The Exposure Draft does not speak to the broader

network of support available through the Trusted Information Sharing Network and the Critical Infrastructure Centre. The Government could provide more details about how the process of assessment and nomination will work and advice on grace periods, the communications approach and the way that industry will be engaged will likely reassure many.

Sharing the Vision of Success

In discussion with many of organisations we work with there are questions around the ability to deliver the reforms and the benefits of doing so. It is important for the Government to share their own roadmap to effectively scale and to support all critical infrastructure operators and a lack of comprehension of the broader scheme as it will roll out to sectors. This is also an opportunity to leverage some of the global precedents in this space and demonstrate benefits. For many critical infrastructure operators, uplifting their cyber maturity so they can meet these obligations is a journey – not a switch that can be "flicked" once legislation comes into place. Many organisations will be launching programs and initiatives in the coming weeks to prepare for this legislation, and the materials published by Government can assist in informing this journey.

Government could usefully include terms and timeframes in such a roadmap and potentially illustrate likely benefits and some of their own plans to improve capacity and capability, as well as real examples of how they have worked with critical infrastructure operators to strengthen the cyber resilience of our nation. We believe there is also an opportunity for Government to leverage lessons learned from other vectors of disruption, including recent examples of bushfires and pandemic, to help inform cyber resilience strategies for industry.

Not all industry entities will be aware of the work that has been conducted by the Department of Home Affairs and ACSC, especially those Industry sectors who have not had significant engagement previously with Government on the topic of Cyber. This could include the previously published guidance material for critical infrastructure sectors, support in cyber incident response, and exercises such as the Cyber War Games. The broad market experience for those that have worked side-by-side with the ACSC and several large organisations tackling cyber problems - generally the experience from these organisations is a positive one.

Final summary

PwC is pleased to support the Government in its endeavour to protect Australian critical infrastructure. The pace with which this risk evolves and the sophistication of the threat actors is driving a necessarily rapid Government response. Naturally the pace is a challenge to achieving optimal outcomes and sustained responses from industry but we note the steps the Government has taken to support and engage with industry to date and going forward. We support the Draft Bill and hope our feedback is useful to achieving fit-for-purpose legislation that will strengthen the future prosperity of our country.