November 24, 2020

Submitted via the Department of Home Affairs online submission form

Department of Home Affairs
Government of the Commonwealth of Australia
[redacted]

RE: Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Coalition to Reduce Cyber Risk, Inc. ("CR2") submits the following in response to the invitation for public comments issued by the Australian Government's Department of Home Affairs ("the Government") regarding the *Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020* ("the Exposure Draft"). CR2 appreciates the opportunity to comment on the Exposure Draft and looks forward to working with the Australian Government to achieve its stated objective of "protecting the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure."

CR2 members include global organizations that represent numerous sectors, including financial services, IT, and telecommunications, that are committed to security, trust, and economic growth and opportunity. CR2 members have deep expertise in cybersecurity and enterprise risk management, as well as unique insights into cross-sector independences and global interconnectivity, which drive the need for consistent, foundational approaches to cybersecurity risk management across sectors and geographies. CR2 has worked collaboratively with public and private sector entities in several dozen countries around the world to advance cybersecurity risk management practices that will both enhance cybersecurity and support economic growth.

As a coalition, we strongly agree with the Government's objectives in putting forward this legislation. We submit the following recommendations in order to further strengthen the Exposure Draft and more effectively meet its objectives.

"Data Storage or Processing" Designation

Understanding that there are commonalities between data centers and cloud services, we believe that the two sectors would be better addressed as separate categories of critical infrastructure. This is in part because the government already has a workable approach to designating data center critical infrastructure, which may be complicated by combining it with that of cloud services.

Additionally, these two sectors face distinct types of threat. For cloud services, one may wish to prioritize the availability of services, whereas for data centers the confidentiality of information may be of greater importance, for instance. Accordingly, we suggest that the Government designate them as separate categories of critical infrastructure.

Furthermore, while we understand that critical infrastructure designation in this sector is not yet complete, the reference to "at least 100 data center entities…and at least 30 cloud service providers" being incorporated indicates that the scope envisioned is too broad. In incorporating so many companies from a single sector, the Government will dilute its own focus and resources, limiting their effectiveness in supporting the most critical entities. Ultimately, if too many entities are 'critical' then nothing is critical.

Register of Critical Infrastructure Assets

While we understand the Government's need for visibility into who owns, controls and has access to critical infrastructure assets, the information requested is often of a sensitive nature. Collectively, this information will represent a high value target for adversaries. We would welcome further information regarding how the Government intends to safeguard such information. Moreover, we would recommend that the collection of information be limited to the extent possible to reduce the potential impact of a cybersecurity incident.

Critical Infrastructure Risk Management Programs

When addressing cybersecurity risks at a national level, a balance must be struck between tailoring mitigation activities to address sector-specific risks and ensuring a nationally coherent strategy that recognizes the inherently interdependent nature of digital systems.

The Government's proposed combination of overarching sector-agnostic obligations and sector specific rules is an effective approach to achieving this. In order to ensure that the two work seamlessly, however, all sectors must be able to discuss risks in a common language, while assessing and addressing them through a common approach. We strongly

recommend the use of international standards for this purpose at a sectoral level, and in particular those with broad industry adoption such as ISO/IEC 27001 and 27101.

Across all sectors, the Government should encourage regulators to utilize ISO/IEC 27101 as the core framework from which to approach cyber risk management. In doing so, they will ensure a common language and approach for across sectors, better enabling cross-sectoral collaboration, which is critical given sectoral interdependencies. Furthermore, leveraging widely used international standards such as these better facilitates international collaboration.

Notification of Cyber Security Incidents

CR2 commends the Government for its proposals to increase information sharing with industry through its development of an aggregated threat picture across critical infrastructure. If we are to adequately defend against ever more sophisticated cyber threats, we cannot afford to silo information that can be used to prevent future incidents. Nevertheless, we are concerned that certain aspects of the proposed approach will inhibit the effectiveness of the Government's efforts.

Firstly, the threshold for reportable *Other cybersecurity incidents* is too low. The description of "attempted access to a network where the entity believes a compromise is imminent" is both ontologically challenging (how can companies be expected to ascertain when a compromise is imminent?) and overly broad, as companies may be the subject of millions of such attempts per day. As a result, the volume of information that is subject to reporting will both overwhelm industry, forcing them to divert valuable resources away from operational activities, and make the aggregation of incident data more challenging. Threat information sharing is valuable only to the extent that it provides security professionals with timely, actionable information. Accordingly, we strongly recommend that attempted access to networks be removed from the scope of the proposal.

Secondly, the timelines for reporting are overly and unnecessarily onerous at 12 hours and 24 hours respectively. The hours immediately after an entity becomes aware of an incident are very challenging from an operational perspective, as company representatives investigate the cause and scale of activities, assess legal ramifications, manage public relations, and ensure the continued confidentiality, integrity and availability of information. Beyond the administrative burden that short timelines for reporting place on critical infrastructure entities, they increase the risk of companies unintentionally sharing information that is either inaccurate or lacks sufficient context to be useful. Rather than mandating arbitrary reporting timelines, we recommend that the Government afford companies flexibility to report when they have relevant information available.

Enhanced Cyber Security Obligations

The structure of the Enhanced Cyber Security Obligations is largely commensurate with the increased risks associated with those entities. For Divisions 2-4, however, it's important that planning, exercises, and vulnerability assessments not be duplicative of activities which have already been undertaken by those entities, without strong reasoning for doing so. Accordingly, the Department of Home Affairs should clearly communicate the purpose of each of these activities and, where Systems of National Significance ("SNS") can demonstrate their existing compliance, they should be granted an exemption in order to avoid finite resources being diverted towards unproductive activities.

Division 5 raises more urgent concerns, particularly with regards to the Secretary's power to "require the entity to install and maintain a specified computer program." Setting aside potential concerns that entities may have with providing the *Australian* Government imposing such a requirement, this would set a very concerning precedent, one which will likely be followed by other, less trustworthy governments. Rather than absorbing responsibility on behalf of an entity that is "technically incapable" of meeting the requirements, we recommend that the Government support capacity building such that the entity is capable of meeting the requirement.

Responding to Serious Cyber Security Incidents

The Government Assistance provisions outlined go further than almost any other developed country in asserting a role for the Government in directing critical infrastructure to take specific measures, or directly intervening in the process itself. The significance of this cannot be overstated and should not be taken lightly, given both its impact in an Australian context and the propensity for other countries to take similar steps in the future.

In Section 35AB the Government has appropriately outlined criteria which narrow the range of circumstances in which these powers can be utilized. The government should go further, however, in outlining clear criteria through which critical infrastructure entities can appeal directives or government action. In the first instance, this could be achieved by entities committing to and proving their ability to implement response and recovery capabilities, as well as to meet incident reporting and other requirements.

Where organizations disagree with the nature of the request, however, there should be a stated authorization for, and a clear, fair process for, the private sector to raise issues associated with such direction or intervention. Thus, if an impacted private sector organization believes that a direction or intervention may pose an unforeseen risk to its customers, then it should be able to pursue a fair process to provide that evidence and challenge the direction and/or intervention authorities.

Given the potential for other governments to implement similar measures in the future, a mechanism should be established for addressing conflicting requirements directives or activities, to ensure that companies are not caught in the middle.

Finally, in order to protect companies from associated legal risks and from being seen as legitimate targets of future cyberattacks, it's critical that these powers not be used to require companies to undertake offensive cyber activities of any kind.

Timeline for Notice & Comment

Finally, while we understand the Government's desire to introduce the Bill in a timely fashion, the three-week time period for public notice and comment falls short of international best practices. This includes the draft *OECD Best Practice Principles on Stakeholder Engagement in Regulatory Policy*,[1] of which the Australian Government is a member, which recommends a 30- or 60-day comment period.

Given the technical complexity of this topic and the significance of the proposals being put forward, we would urge the Australian Government to extend the deadline in order to better facilitate stakeholder input on the Exposure Draft.

Respectfully Submitted,

The Coalition to Reduce Cyber Risk, Inc.

CC: Alex Botting, Venable LLP

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