1st December 2020

Australian Cyber Security Centre (ACSC)
Department of Home Affairs
CANBERRA, ACT

Lodged online

Dear Sir/Madam,

RE: EXPOSURE DRAFT OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL

Thank you for the opportunity to make this submission on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill,* and the accompanying Explanatory Document.

For the purposes of this submission, we have limited our comments to our expertise as Australia's national standards body, and discuss specific proposals outlined in the Exposure Draft. We thank the Department, and broader agencies engaged in these reforms, for their engagement to-date. We look forward to ongoing engagement to ensure that any implementation decisions are beneficial to both government and industry. We do share the view that clarity on any regulatory approaches proposed, including the implications and costs thereof, is important prior to the enactment of comprehensive legislation.

1. Proposed Positive Security Obligations

We note the Government's intention to establish Positive Security Obligations (PSO), with respect to specific identified sectors, through sector-specific rules, with implementation subject to a quantitative Regulatory Impact Statement at a later date.

In relation to the proposed requirement for a risk management program, we look forward to engaging with the Australian Government on this process. We note, and welcome, the ability the Bill would establish, under section 30AH, to leverage Australian adoptions of ISO and IEC Standards, or indeed Australian Standards published by Standards Australia, for this purpose. As we have previously outlined, whilst uptake of standards in respect of information security and cyber security more broadly, can be variable, many responsible companies and entities do adopt recognised international standards as part of mature risk management processes. Recognising proactive adoption and use of such standards, through any proposed new risk management program requirement, is important. Additionally, this might incentivise good practice that aligns with international supply chains, ensuring a heightened, and more integrated, baseline defensive posture. We are of the view that this requires deep industry engagement and are ready and willing to play a supportive role.

In this respect, we welcome the Government's commitment, as expressed in the explanatory document, to *"continue to work with industry and state and territory governments to make sure that existing regulations, frameworks and guidelines are leveraged, and to minimise any duplication or unnecessary cost burden."*[1]

2. Legislative timeframe

We are cognisant of the multiple reviews underway in areas relating to digital issues, ranging from privacy to cyber security to emerging technologies, and with legislative implications in some of these areas. For this reason, we recommend thorough dialogue prior to consideration by Parliament of this Bill to ensure there is clarity around sector specific rules, infrastructure and relevant costs, which would be central to any proposed Regulatory Impact Statement and practical implementation.

---

[1] Department of Home Affairs (2020). *Security Legislation Amendment (Critical Infrastructure) Bill Explanatory Document*. Canberra: Commonwealth of Australia, p.9

Further contact

For any questions or further information on the matters raised in this submission, please contact Dr Jed Horner, Strategic Advocacy Manager, at [redacted] or via phone on [redacted].

[redacted]

Yours sincerely,

Daniel Chidgey

Head of Stakeholder Engagement