ABSIA Australian Business Software Industry Association

217 Flinders Street
Adelaide SA 5006
info@absia.asn.au | www.absia.asn.au

12 February 2021

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

Via online form.

Dear Committee Secretary,

Re: ABSIA's Submission to Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018.

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of our members and the software industry.

Overall, ABSIA supports the expansion of critical infrastructure to include more critical assets across a wider range of industries. COVID-19 and the consequent impacts of people working from home and a heavier reliance on certain sectors and their networks has highlighted the importance of widening this definition. For example, the Single Touch Payroll network has been fundamental in supporting the JobKeeper and JobMaker initiatives.

We understand that much of this work is still in its early stages and ABSIA looks forward to working with the Government and regulators as these changes are implemented. The following paragraphs outline some concerns arising from the Security Legislation Amendment (Critical Infrastructure) Bill 2020 - Explanatory Memorandum and associated material about the review along with issues identified within the industry.

While some industries have been making significant progress with improving their cyber resilience, think APRA's CPS 234 and the ATO's Operational Framework, other industries have lagged behind, meaning these changes will be quite significant to implement. It is important to note the change management, costs and time that will be required to operate in line with these changes. Further, any changes to security requirements, as a result of assets being impacted on by the proposed legislation, should be done in consultation with the appropriate industry and its representatives.

We understand that the Government is not intending to offer financial support to critical infrastructure owners and employers so that they are able to meet these proposed reforms. While education and training is expected to be offered through the TISN, more thought needs to

be given to making these costs affordable for smaller organisations that may interact with or own a critical infrastructure asset.

Where the Government decides to intervene in a cyber incident, then it should be clear who takes responsibility for the consequences of actions taken during that intervention. It would be unacceptable for the participants and/or owners of critical infrastructure to have to bear the responsibility for actions taken by the Government during an intervention. Outlining this in detail will assist in giving the industry confidence in this process and enable them to better understand the Government's role if they should intervene. Further, it should be made clear early on whether funding will be available to critical infrastructure assets to assist in their recovery after a cyber incident, especially where the Government has intervened.

ABSIA would appreciate the opportunity to engage further on the points laid out in this submission. For further information, please contact [redacted].

Yours faithfully,

[redacted]

Simon Foster,
President & Director
Australian Business Software Industry Association, Limited.