

26 August 2021

Hon Karen Andrews MP  
Minister for Home Affairs  
Parliament House  
Canberra ACT 2600

via email: [Karen.Andrews.MP@aph.gov.au](mailto:Karen.Andrews.MP@aph.gov.au)

Dear Minister

### **Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020**

I am writing to you on the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**SOCI Bill**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 46,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits, large and small businesses and the government sector.

I appreciate that submissions to the PJCIS review have closed however it has come to the AICD's attention that the current drafting of the SOCI Bill may inadvertently expose some employees, contractors and directors of regulated entities to liability in certain circumstances.

The AICD has had the benefit of reviewing the Law Council of Australia's submissions on this issue, and is writing in support of the Law Council's recommendation that immunity be expressly extended to cover all participants involved (including directors and officers of related body corporates) and all conduct, acts and practices undertaken to comply with the Act.

### **Limitations of proposed statutory immunities**

The AICD supports the broad objectives of the SOCI Bill to build on the existing regulatory regime under *Security of Critical Infrastructure Act 2018* (Cth) (**the Act**) to enhance the security and resilience of critical infrastructure assets and systems of national significance.

A key arm of SOCI Bill and the expansion of the Act is the proposed ability of the Minister to authorise the Secretary of Home Affairs to give directions to an entity to take action or provide something. We understand from the Explanatory Memorandum that giving directions to an entity would be utilised in rare emergency circumstances, as a matter of last resort and limited to responding to the cyber security incident.<sup>1</sup> In the context of the considerable scope of the directions provisions and the seriousness of any situation that would warrant government intervention our view is that protections for employees and officers of the impacted entities need to be comprehensive.

---

<sup>1</sup> Explanatory Memorandum, paragraph 866.

We are concerned that as currently drafted the immunity provided under subsections 35AAB(2), 35AW(2), 35BB(5) and 30BE(2) is too narrow through limiting protection to 'employees, officers or agents' of the entity. While 'officer' will generally capture directors of an entity the current drafting may create uncertainty about application to directors, employees or contractors of a related entity and/or who sit within a group structure. In the expanded list of critical industry sectors, it is common for entities to have corporate structures where key services and support are provided by related entities. As currently drafted, a director of a related entity may be exposed to personal liability in the event the related entity assists the entity comply with a direction under the Act. The personal liability may arise due to the assistance bringing about a conflict with the director's obligations under the *Corporations Act 2001* (Cth).

While the risk of such director personal liability materialising in these circumstances may appear small it is important to consider it within the context of the Australian director liability environment. In 2019 the AICD commissioned leading law firm Allens to evaluate the frameworks for imposing criminal and civil liability on directors in Australia and comparative jurisdictions (being the United Kingdom, New Zealand, Canada, Hong Kong and the USA). The findings of the Allens' analysis found that Australia's director liability environment is 'uniquely burdensome'.<sup>2</sup> We would be happy to provide further information on this research if it would be of assistance to your office in considering this issue.

The AICD supports the Law Council of Australia's proposal that more expansive immunity provisions could be modelled on section 70AA of the *Banking Act 1959* (**Banking Act**).<sup>3</sup> Importantly the immunity provisions of the Banking Act explicitly cover officers of related body corporates, including within a group structure.

Comprehensive immunity will assist the operation of the Act through providing comfort to senior decision makers of entities, including directors, that there is appropriate protection if complying with an obligation or direction under the Act results in conflict with other obligations and duties. This comfort will avoid delays or barriers to an entity and its directors responding to a critical cyber incident and complying with directions from the Secretary of Home Affairs.

### Next steps

We hope our response will be of assistance. Our Head of Government Relations, Matt Pritchard, will be in contact with your office to ascertain if any further information is required. Matt can be contacted on MPritchard@aicd.com.au or I can be reached directly on LPetschler@aicd.com.au.

Yours sincerely,



**Louise Petschler GAICD**

General Manager, Advocacy

---

<sup>2</sup> AICD commissioned research: Australia's "uniquely burdensome" director liability environment. <https://aicd.companydirectors.com.au/-/media/cd2/resources/advocacy/policy/pdf/2020/aicd--advice-for-publication-including-organograms.ashx>

<sup>3</sup> Law Council of Australia, Submission Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Review of the Security of Critical Infrastructure Act 2018 (Cth), 17 February 2021, page 91.