STATEMENT BY THE AIIA CEO RON GAUCI ON REVIEW OF THE *SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE)* BILL 2020

Thank you for this opportunity to appear before the Parliamentary Joint Committee on Intelligence and Security as part of your Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

The AIIA represents a diverse group of members in the digital ecosystem, including global, multinational, national and SME entities. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

As expressed in our submissions to the Department of Home Affairs and the Committee in 2020 and 2021, the AIIA has indicated its support for the expansion of sectors that are defined in this bill as critical infrastructure sectors and fall under this regulatory scheme. The Department of Home Affairs' 2020 review of critical infrastructure (CI) and the preceding consultation paper recognised the digitisation of our economy and resultant increase in cyber threats.

We acknowledge that the government is seeking to extend a regulatory framework across 11 critical sectors and their attendant systems in order to protect key supply chains and infrastructure of national importance in the event of a serious security threat, and understand the rationale. The AIIA acknowledges the significance of CI legislation as a policy response for the defined critical sectors, with oversight in terms of their cybersecurity sending a strong market signal and driving investments accordingly for those cloud and other sectors in line with this policy direction.

However, the AIIA calls on government and the Joint Committee to ensure that the Critical Infrastructure regime operates on the basis of rules that are genuinely co-designed, flexible, and give rise to regulation that is not burdensome or duplicative in nature.

Any action taken by the Government through the Department of Home Affairs or the Australian Signals Directorate in relation to critical infrastructure entities in the event of a cybersecurity incident could have reputational impacts as well as impacts upon customers, which needs to be considered in analysing downstream effects of declarations and interventions.

Under the data storage and processing sector being defined as a CI in the legislation, AIIA members are concerned that their customers have their own security obligations, which they may seek to pass onto them as the storage or cloud technology infrastructure entity. The impact of this legislation and obligations need to be considered by the sector, as well as ensuring that customer contracts address potential implications of the reforms, e.g., the potential need for the entity to provide access to their infrastructure to the Australian Signals Directorate, which could have contractual implications upon customers. These impacts and appropriate remedies should be considered by the Committee.

Regarding the direct action power in regards to the data and processing sector, the AIIA is calling for appropriate appeal mechanisms, the opportunity for judicial review, and the ability to refer disagreements to an independent expert panel to ensure appropriate recourse. The AIIA submits that further guidance, clarity on the scheme's remit and reach as well as oversight mechanisms are required to ensure both industry support as the regime is implemented and that the scheme is fit for purpose and achieves the government's stated ambitions.

Ron Gauci, AIIA CEO