October 14, 2021

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

Dear Minister,

The undersigned associations, which represent hundreds of technology and technology-enabled companies, respectfully submit this letter on behalf of our member companies regarding the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, hereafter "the Bill." Our members share the Australian Government's commitment to protecting Australians and Australia's critical infrastructure against cyber threats. However, the Bill remains highly problematic and largely unchanged despite extensive feedback from our organisations. Without significant revision, the Bill will create an unworkable set of obligations and set a troubling global precedent.

We are disappointed by the recent report from the Parliamentary Joint Committee on Intelligence and Security (PJCIS)[1], which recommended that the elements of the Bill which caused the most concern for industry stakeholders – namely the government assistance powers granted under Part 3A and incident reporting obligations -- be fast-tracked and pushed through as a separate Bill, without further public consultation. As representatives of member companies that include both Australian and international companies, we urge the Australian Government to reject this recommendation and to seriously consider our recommendations below.

As drafted, Part 3A of the Bill provides the Australian Government with information-gathering, direction and intervention powers that are not subject to reasonable due processes, which would normally allow affected entities to appeal or have these decisions independently reviewed.[2] While the Government asserts that this power is intended only as a measure of last resort to address "cyber security incidents," the Bill provides the Government with unprecedented and far-reaching powers, which can impact the networks, systems and customers of domestic and international entities, and should be subject to a statutorily-prescribed mechanism for judicial review and oversight.

We are also concerned by the global impact that such a Bill will have and how it undermines the values that Australia promotes internationally. The Australian Government has been a global

[1] Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 dated September 2021.

[2] We note there are limitations in judicial review under 'original jurisdiction' of this Bill and that independent operational oversight from organisations - such as IGIS and the Ombudsman - is no substitute for ADJR Act review.

leader in policymaking around technology and security, specifically addressing threats posed by companies that may be subject to extrajudicial direction by a government. The signal sent by these measures is that these rules do not apply to Australia. This undermines the Government's good work internationally on these issues and sets a disturbing precedent for other governments facing similar national security challenges. We strongly recommend the Australian Government amend the Bill to provide for a statutorily prescribed right of appeal and review of the Part 3A powers.

In addition, we once again reiterate our recommendation that the mandatory cyber incident reporting timeline be extended from "within 12 hours" to "at least 72 hours" or "without undue delay." The mandatory 12-hour reporting timeframe diverges from global best practices and will inhibit our ability to focus on truly critical incidents. Additionally, we recommend removing the requirement to report "imminent" cyber incidents. Our member companies would collectively block millions of threats a week; if required to report these the Australian Government would likely be inundated with data. The current reporting requirements of the Bill will likely lead to the reporting of inadequately contextualized information or misinterpretation of the event in a situation where accuracy is of great importance, which will not provide useful or actionable information to the recipient government entity.

Given the above, we once again reiterate our request that the Government reconsider its proposed path forward immediately on these two issues and address the significant concerns raised by industry. Our member companies prioritise cyber security, both within our own businesses and for our customers, and we support the Australian Government's goal to improve cyber security in Australia. However, these two proposals would not accomplish that goal, would have significant unintended consequences that would decrease security in practice, and would set dangerous global precedents.

We strongly urge the Australian Government to consider the precedent the Bill sets for Australia's trade partners in addressing national security risks, as well as the challenges Australian companies may face in other markets if these requirements are replicated by other governments. We greatly appreciate your attention to our concerns and your consideration of our recommendations, and we look forward to continuing to work with the Australian Government as it seeks to reform laws on critical infrastructure cybersecurity, especially in shaping the proposed Positive Security Obligations to be aligned with international standards.

Sincerely,

Information Technology Industry Council
Australian Information Industry Association
Cybersecurity Coalition