Atlassian's Submission in relation to the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Department of Home Affairs
ci.reforms@homeaffairs.gov.au

27 November 2020

We appreciate this opportunity to provide input on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the **Bill**).

At Atlassian, we build enterprise software products to help teams collaborate, including for software development, project management and content management. As a digital-first company, we know the critical role that security and resilience play in ensuring the integrity, privacy and trustworthiness of our own products and services.

We also understand that this is not just an issue for the tech sector. Australia's essential services and critical infrastructure are increasingly digitised, increasingly interconnected and increasingly targeted by malicious actors, trends that have only accelerated this year. We therefore strongly support efforts that seek to uplift security capability, foster better cybersecurity practice and improve resilience across the economy. However, in order for these efforts to succeed – and for the public to have confidence in them – they must be implemented in a collaborative way that is open, fair and as clear as possible for all stakeholders to understand. We are concerned that, in its current form, the Bill does not always meet these standards.

Atlassian is supportive of the proposed approach to the implementation of the Positive Security Obligation outlined in the Bill and explanatory materials. We appreciate that the materials clearly acknowledge the importance of government and industry partnerships to the implementation of these reforms and we recognise the need to foster better collaboration and information sharing.

We strongly agree that the specific requirements for each sector should be the subject of extensive further consultation and co-design in order to ensure that they:

- are clear, proportionate and targeted towards the outcomes they are trying to achieve;
- have careful regard to any overlapping or conflicting requirements that may already exist in and across relevant sectors; and
- impose the least burdensome measures to achieve the proposed security outcomes.

However, further attention should be given to whether these aims are met in the Bill itself, not just the rules to be subsequently made under it. We are concerned that this is not always the case, especially due to the extremely short period for consultation on this Bill, which represents the first opportunity for stakeholders to review, understand and comment on the substantive details of these reforms.

Our concerns with the Bill arise in three key areas: clarity, fairness and transparency. We believe that these elements are fundamental to ensuring not just the effective and proper operation of these reforms, but also public confidence and trust in the government as well as in our essential services and critical infrastructure.

In order to best address these concerns, we submit that these important reforms should, in all respects, align to the following core principles:

1. **The scope of the sectoral application of the scheme should be as clear as possible.** This is critical to ensure that industry can be confident about whether or not they will be subject to its requirements. One example of how this principle would apply to the current Bill is in defining the scope of the "data storage or processing sector" and relevant assets falling within it. The Bill itself does not define "data processing" or a "data processing service", and further, does not clarify when an asset will be considered to be used "wholly or primarily" in connection with a data storage or processing service.

   The explanatory materials state that an asset will not qualify where data storage is simply a "by-product" of providing a service, but do so while also noting that the sector could cover software-, platform- or infrastructure-as-a-service solutions. The broad range of solutions provided by SaaS, PaaS and IaaS providers mean that their services could fall anywhere along a broad spectrum of data processing and storage, more than "by-products" but (perhaps) less than "wholly or primarily" providing such services. This lack of clarity, which was noted in a number of submissions on the earlier concept of the "data and the cloud" sector in the Consultation Paper, has remained notwithstanding the more detailed drafting in the Bill.

2. **Strong review and oversight mechanisms can and should be available.** We appreciate that the powers described in Part 3A of the Bill are intended to ensure that Australia's essential services and critical infrastructure, and those responsible for them, are best able to respond in the event of a serious cyber security incident. However, these exceptional circumstances and the significance of these powers should emphasise, rather than lessen, the need for strong oversight and review of their exercise in order to ensure that they continue to function properly and effectively into the future. We are accordingly concerned that:

   - The Bill does not permit judicial review under the *Administrative Decisions (Judicial Review) Act 1977 (Cth)*, or any form of merits review or other appeal mechanism. We note that the explanatory materials consider this

exclusion to be appropriate based on other national security or foreign interference legislation, or because of the potential delays that these processes could introduce. However, we strongly believe that this cannot and should not hinder the introduction of such mechanisms in this Bill. The circumstances in which these powers will be exercised -- which must meet a seriousness threshold, and often involve highly sensitive and technical matters -- are similar to those under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, and we reiterate our position (supported by the recommendations of the Independent National Security Legislation Monitor) that these merit strong independent oversight and review.

- The Bill does not provide for periodic review by either or both of the Parliamentary Joint Committee on Intelligence and Security or the Independent National Security Legislation Monitor once passed. This is an important way for the government and the public to consider and revisit these measures after their implementation, to ensure that they continue to meet their aims, and should be incorporated.

3. **The guardrails in place for the exercise of these intervention powers must be robust.** This is particularly the case because the breadth and technical nature of these powers are such that there is significant potential for unintended consequences to arise. We appreciate that the Bill seeks to include "stringent safeguards and limitations" for the exercise of powers under Part 3A. However, we believe that there is significant scope to further consider and improve these. For example:

   - The Bill often requires the Minister to be "satisfied" of certain matters, and requires the Minister to "have regard to" certain matters in making such determinations. These criteria can and should be more objective in nature, including (where relevant) by clarifying the weight to be given to those matters that must be taken into consideration. The Bill should also be clear that Ministerial direction should only be used as a last resort in areas of wilful and consequential non-compliance with requests for cooperation (for example, by implementing a "tiered" approach whereby a form of "action request" must be issued, and not complied with, in advance of any authorisation).

   - We recommend that the government consider establishing sectoral rules to guide and limit the scope of Ministerial directions as they will and may apply to each sector as part of the proposed regulatory co-design process. These rules should be based on a shared understanding of industry and government capability and pre-established engagement protocols.

   - Under section 35AD, consultation is required in respect of action directions and intervention requests unless such consultation may "frustrate the effectiveness" of the authorisation. We appreciate that these powers may need to be exercised in situations of emergency or other cases where

consultation may either be difficult or unnecessary. However, many of these authorisations are likely to be highly technical in nature, such that prior technical consultation and expertise may not only be beneficial but indeed necessary in order to avoid unintended consequences.

Atlassian is committed to working with the Government, industry and other stakeholders on these and other issues to ensure that the Bill reflects the type of clear law and fair procedure that will best position Australia for the future.

Yours sincerely,

Patrick Zhang
Head of IP, Policy & Government Affairs
Atlassian

David Masters
Director of Global Public Policy
Atlassian