ATLASSIAN

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

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

12 February 2021

We appreciate this opportunity to provide input to the Committee on 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 in the past 12 months. 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.

Earlier this year, Atlassian published eight Principles for Sound Tech Policy, which are attached to this submission. These Principles are intended to not only guide Atlassian's own engagement on important matters of public policy, but to set forth guiding principles for what we believe sound technology-related public policy should look like more broadly.

Analysing the Bill against our stated principles, our concerns arise in three key areas: clarity, proportionality 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.

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, as per our fourth principle [*consult early, consult often*], 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.

We also recommend that this consultation process recognise the unique characteristics of the "data storage or processing sector" as a set of horizontal, enabling technologies rather than a more traditional, vertical "sector" (as also noted in our comments on this sector below). It would therefore be inappropriate to define sector specific rules for "data storage or processing" without first understanding the existing relationships and technical and regulatory interdependencies with the other proposed critical infrastructure sectors. The sequencing and prioritisation of the consultation process should take this into account, to ensure that any consultation on this more horizontal sector has the benefit of preceding consultations with these vertical sectors.

In order to best address these concerns, we submit that these important reforms should, in all respects, address the following themes, aligned to Atlassian's principles:

1. **The scope of the sectoral application of the scheme should be as clear as possible.** In line with Atlassian's first principle [*Define the playing field*], it 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 or processing 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 Department of Home Affairs' earlier Consultation Paper on these reforms, has remained notwithstanding the more detailed drafting in the Bill.

2. **The guardrails in place for the exercise of these intervention powers must be robust.** As outlined in our second principle [*Engage with the issue*], the complexity of the interdependencies across the technology environments of critical infrastructure operations, combined with 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 Ministers to be "satisfied" of certain matters, and requires the Ministers 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.

3. **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, aligned with our fifth principle [*Let the light in*] 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.

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.

David Masters

Director of Global Public Policy
Atlassian

Atlassian
Public Policy

Atlassian Principles for Sound Tech Policy

Table of Contents

Atlassian Principles for Sound Tech Policy

Preamble

We at Atlassian are strong believers that the future of human endeavour and economic prosperity will increasingly flow from innovation and technology. And as 2020 has shown us, ever-greater digitisation is not only tomorrow's trend, but also today's urgent requirement.

But the pace of technology development means that all of us – individuals, private industry and government – must together develop policy frameworks that unleash the positive potential of technology for society while reducing any negative effects.

We know that developing a sound policy framework requires carefully considering the interests and rights of all vested stakeholders, as well as the potential impacts on them. This complex undertaking requires dedicated planning and process--as well as guardrails for the ultimate result. It is not surprising then that sometimes such policy efforts come up short of their intended aims.

This is why we think it is time for a reset on the conversation around tech regulation--one that fully encompasses the positive contributions of the tech sector to society, the legitimate regulatory requirements of government and protection of individual rights, as well as the need for a consistent and reliable environment for shared economic prosperity.

To contribute to this renewed conversation, Atlassian offers the following set of guiding principles to help government, industry, and the public converge on the essential qualities of sound regulation in the technology sector. If implemented, we believe that these guiding principles will result in targeted and proportionate policies, informed by a collaborative process, that ultimately unleash the positive potential of technology while fully addressing individual and societal interests – a true "win win" outcome for all of our communities.

Lastly, as these Principles make clear, we believe that collaboration is key to sound tech policy. As part of our drafting process, we engaged with numerous members of the tech sector, industry associations, and civic organizations who share our common vision. But to ensure that collaboration and improvement can continue even after publication, we are licensing these Principles under a **Creative Commons** license, so that others can adopt, modify and build upon these ideas as the dialogue continues.

Atlassian Principles for **Sound Tech Policy**

I. Define the playing field

Sound tech policy should have clear objectives. This means that everyone should be able to understand the specific problems that regulation seeks to solve, or the interests it seeks to support. More importantly, the regulatory solution should be clearly targeted at that identified problem. Unclear intent breeds distrust and concern.

II. Engage with the issue, don't dumb it down

Sound tech policy should be developed with a clear understanding of the relevant technology. Lawmakers and regulators may not all be technical experts, but if they engage with these experts and other stakeholders to understand the relevant technology and business models, they will be better positioned to respond to them through regulatory means. This can assist in identifying which regulatory means can be used effectively, and which ones are impractical or overly burdensome.

III. Treat the ailment, don't kill the patient

Sound tech policy should be proportionate, and should always seek to minimise unintended consequences. If regulatory responses are not properly considered and tested, they can overreach or lead to unintended and undesirable consequences. These consequences can be just as devastating to companies and their users as failing to act at all. Regulations should be surgical; government should not use a regulatory hammer where a scalpel is appropriate for its goals.

IV. Consult early, consult openly

Sound tech policy should be developed through open, consultative processes. When all relevant stakeholders are engaged early in regulatory processes, potential risks and unintended consequences can be identified and addressed before decisions are made. Open engagement also fosters greater trust in regulatory processes and creates space for both sides to clearly state their objectives or concerns. Early and extensive consultation is an obvious way to try to mitigate against a lack of understanding of the relevant technology or the business model of companies, and the consumer use cases. It also helps governments to ensure that regulations are as effective as possible.

V. Let the light in

Nothing is more uncertain than "black box" exercise of government discretion outside of the public eye. Sound tech policy should provide for transparency in government decision-making and set forth fair procedures that allow meaningful challenge of and detailed inquiry into those decisions.

VI. Address behaviour, don't punish success

Sound tech policy should seek to mold and target behaviours across a sector or drive outcomes on a systemic basis. It should not target specific individuals or companies. An approach that singles out individual organisations does not take into account the diversity and dynamism of the tech sector. More importantly, such an approach is not a sound long term approach addressing future challenges. This does not stop laws from ultimately being enforced in relation to identified individuals or entities, but regulations should not be made out against them specifically in the first place.

VII. Tech (and trust) is global

Sound tech policy should be coherent and consistent, mindful of global standards and able to enhance global interoperability. Local conditions must of course be considered, ensuring that any regulation forms part of a coherent local landscape. However, if competing regulatory frameworks are not also considered, there is a high risk that technology regulation will develop in a piecemeal manner that increases the burden on innovation, business, and consumers alike.

VIII. Build the foundation for shared success

Sound tech policy should provide a consistent and reliable framework for business and investment. We fully appreciate and support governments' legitimate interest in meeting regulatory goals and protecting consumers and the public, and the responsibility that all businesses share to ensure that this is achieved. It is equally important that the legislative process and outcome should be measured, fair, and reliable, in a manner that provides business stakeholders with the confidence to grow and invest in jobs, infrastructure, and improved products and services for their customers.