ATLASSIAN

Atlassian's Supplementary 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

8 July 2021

We appreciate the opportunity to continue to engage with you in this important review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the **Bill**).

This supplementary submission reflects the core themes of, and further builds upon, Atlassian's submission to the PJCIS relating to the Bill on 12 February 2021 (our **First Submission**).

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 fully understand and appreciate the absolutely critical role which security, safety and resilience play in ensuring the integrity, privacy, reliability and trustworthiness of our own products and services and our own customers' data.

We consider it an important part of our role to highlight the views of our employees and customers, and also our fellow technology sector colleagues who may not have the resources to directly engage themselves in these processes.

In addition to our First Submission, we would like to emphasise the following key themes:

1. The Bill should recognise and take account of pre-established engagement protocols.

Given the complexity of the interdependencies across the technology environments of critical infrastructure operations, and the breadth and technical nature of the powers contemplated in the Bill (in particular Part 3A), there is significant potential for powers to be used in a way that does not acknowledge the technological landscape (and limitations) and undermines their effectiveness.

We note that the Government consultation of the data processing and storage sector, which commenced on 29 June, focuses on the co-designing of sector specific rules for the implementation of positive security obligations but will not address other aspects of the Bill, including the Government assistance power.

While we still believe, in line with our First Submission, that the Bill should allow for judicial review of Government assistance powers, at a minimum we think that as part of the co-design process, government and industry should jointly develop pre-determined, "ready for action" protocols for each industry. Given the significant and individual technical complexities involved in the delivery of services across the "data storage and processing sector", individual company protocols should also be countenanced within our sector.

These protocols would inform the exercise of the government's power and allow all stakeholders to have a more thorough understanding of their responsibilities when powers are exercised. The Bill should also recognise and accommodate these protocols to ensure that they are practically effective. This could be implemented by the following amendments:

- As part of the consultation process under s 35AD (relating to action directions and intervention directions), or other relevant points before making a ministerial authorisation, the Minister must give due regard to the protocols to inform the nature and extent of the authorisation.

- Any direction (for example an action direction under s 35AQ) may be made with a condition that it is complied with in accordance with relevant applicable industry protocols.
- Adherence with a protocol may be used as an element by which an entity may demonstrate compliance with a direction.

Creating protocols and recognising them in the Bill provides benefits for all stakeholders:

- Government will have greater capability, supported by industry knowledge, to quickly and effectively carry out ministerial directions under the Bill in a way which achieves the objectives of the direction without being hindered by protracted technical consultation or planning when an event occurs.
- Speed and agility are enhanced when an issue or event arises.
- Companies can more easily explain to customers and stakeholders the practical consequences of powers under the Bill by reference to draft protocols which will be more detailed than the broad powers in the Bill.
- Companies and industry bodies will be incentivised to engage in the planning process if they are given the opportunity to co-design protocols which are tailored to the industry and acknowledge the unique circumstances and operating environment of that industry and its participants.

2. **The notification threshold for the seriousness of an incident should be higher.**

Part 2B of the Bill addresses notification of cyber security incidents, for both “critical” incidents and “other” incidents. As noted in the Explanatory Memorandum, we appreciate that government is concerned with capturing broad trends in cybersecurity incidents which it can feed back to industry. However, the usefulness of the data will be limited if the materiality threshold is too low and the government receives too many reports. The ACSC noted in its Annual Cyber Threat Report (July 2019 to June 2020) that it received 164 reports per day, or one report every 10 minutes. There is a risk that government is overwhelmed by incident reports and both government and regulated entities have a significant additional administrative burden which is not necessary.

Atlassian’s view is that the “Other incidents” reporting requirement (section 30BD of the Bill) should not apply to incidents which “are imminent” or incidents which are “likely to have a relevant impact on the asset”. Many regulated entities are subject to an extraordinary number of attempted cyber-attacks which, if successful, would be likely to have a relevant impact on them. We think that a more appropriate balance – and more meaningful data – is for government to receive reports for cyber incidents which are happening, or have happened, and which have actually caused a material impact. This view aligns with the more limited position taken in the EU NIS Directive (Directive 2016/1148) which requires reporting for an “incident having a substantial impact” on the provision of various services. The Directive also defines the term “incident” with a high materiality threshold, being “any event having an actual adverse effect on the security of network and information systems”.

If broader data collection is still deemed necessary, low materiality events could be provided to government on a high level and aggregated basis over longer reporting horizons (e.g. quarterly).

3. **The co-design process should acknowledge the diversity of the data processing and storage industry and its “supporting role” to other industries.**

As noted in our First Submission, the consultation process should recognise the unique characteristics of the “data storage and processing sector” as a set of horizontal, supportive technologies rather than a traditional vertical sector. It is critical to understand the interdependencies between the data sector and the other critical infrastructure sectors it supports as regulation of those other sectors will necessarily “flow through” to the data sector.

Accordingly, to avoid overlap between sector requirements and to appropriately address the complexity in the data sector relationships:

- The data sector should be dealt with last in the consultation process. Noting that government is imminently starting the co-design process for the data and processing sector next week and it may not be appropriate to delay at this stage, we are concerned that the timing may not enable proper consideration of the overlapping obligations between data sector providers and their clients (which operate across all other sectors). We suggest that there should be a further opportunity to comment on the proposed rules for the data sector before the passage of the Bill to leverage knowledge gained in the consultations with other critical infrastructure sectors; and
- For companies within the data and processing sector, the data and processing rules must clearly take precedence over the rules of other critical infrastructure sectors. It would be unworkable for companies like Atlassian, as a downstream service provider, to be subject to the requirements of each other critical infrastructure industry. Likewise, companies in other sectors will need clarity that Atlassian’s compliance with the data sector rules will not have the consequence that they are failing to comply with their respective sector rules.

Atlassian is committed to continued engagement with the government, industry and other stakeholders on this Bill.

David Masters

Director of Global Public Policy
Atlassian