The Hon. Peter Dutton, MP
Minister for Home Affairs
Department of Home Affairs,
Australian Government.

27 November 2020

Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 - Submission

Dear Minister Dutton,

Thank you for the opportunity to provide submissions on the *Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020*, associated *Exposure Draft of the Intelligence Services Regulations 2020*, and accompanying documents.

We have set out those submissions on the following pages, starting with an 'Introduction' and then 'Submissions' on specific sections of the Bill. We have not made submissions on the *Exposure Draft of the Intelligence* Services *Regulations 2020*.

I would like to take the opportunity to commend your Department for issuing the Bill, as it may be the most important recent step forward for Australia to have an opportunity to develop significant sovereign capability with much needed Government guidance, oversight and regulation, to ensure enduring and resilient cyber security for the nation's critical infrastructure assets.

Yours sincerely,

[redacted]

Rupert Taylor-Price
Chief Executive Officer

Overview of Vault Cloud®

Pioneered and founded in 2012, Vault Cloud was developed with security at its core, embedding Australian Government security controls natively into the Cloud platform. We have designed, built and automated the delivery of Australian Government security controls to create one of the world's most secure Clouds. Government organisations can now deploy services faster and securely, with flexibility and at hyperscale.

We are Australian owned and operated, and the first Cloud platform globally to be certified by the Australian Signals Directorate to process and store classified data.

On 30 June 2020 we signed a whole-of-government agreement with the NSW Government - which was a first for an Australian company.

Our CEO and founder Rupert Taylor-Price has recently been appointed to the board of directors with the AIIA and is also part of the newly created ICT/Digitial Sovereign Procurement NSW Government Taskforce.

We have a wealth of knowledge and experience within our board of directors including Jane Halton who has held positions in many Australian Government Departments, including Secretary of the Australian Department of Finance and now holds director positions including the independent non-executive director of ANZ, independent chair of the council of the Ageing, a non-executive director for Clayton Utz and a council member of the Australian Strategic Policy Institute.

Vault submissions on the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Delivered by electronic upload:
https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems/submission-form

Introduction

Cyber security assurance for a nation's critical infrastructure is to a large extent determined by the nation's positioning on sovereign capabilities in this area. It is also determined by a nation's ability to oversee and where appropriate regulate such capabilities (with a view to further strengthen sovereign capabilities through regulation).

As Vault has mentioned in a previous submission regarding sovereign capability, a fully sovereign capability, or the one that gets closest to this approach, is the preferred model for maximising security capabilities in government and critical industries.

A nation can adopt an approach to the oversight and regulation of cyber security capabilities for critical infrastructure that ranges between (i) no oversight or regulation, to (ii) Government guidance, oversight and regulation of private critical infrastructure assets, to (iii) authoritarian Government ownership or regulation of such assets.

In our view Government guidance, oversight and regulation of private critical infrastructure assets is the preferred model, and can increase sovereign capability and therefore increase cyber security assurance for Australia's critical infrastructure assets.

Having no or low domestic capabilities will make Australia dependent on and beholden to the interests, standards and requirements of a small number of foreign global suppliers. Vault in a previous submission referred to this scenario leading to an Australian cyber security 'black swan' event. Government over time then also may find it necessary to declare certain critical data storage or processing assets of these foreign suppliers as 'systems of national significance'. In Vault's view their foreign interests and global business models make it highly likely that they will resist meeting, or not be able to meet, all the Government's associated guidance, policy and regulatory requirements.

In the last ten years the data storage and processing sector has not only become a critical infrastructure ('CI') sector in its own right but has permeated into all other CI sectors. If it has not already, the data storage and processing sector will likely become the most critical CI sector in the near future. Yet today it stands unregulated and without a regulating body. Fundamentally the commercial interests of the sector and the national security interests of Australia may not be fully aligned at all times. The combination of the importance of the sector and the alignment risks gives rise to an urgent need for regulation. The legislation is a positive first step and the sense of urgency is appropriate, however further progress will be needed for the data storage and processing sector.

In the submissions below we have made proposals that we are hoping will further enhance and strengthen the two key requirements of (1) sovereign capability, and (2) oversight and regulation.

Submissions

1. **Critical infrastructure assets located outside Australia - section 9(2B)**

   Now that 'critical data storage and processing assets' are included in the list of critical infrastructure, consider whether this subsection might exempt certain components of such assets from the Government's regulatory framework, where that was otherwise not the intent.

   Vault in any event recommends that for certain Government and critical infrastructure workloads, the best position would be to use fully sovereign data storage and processing assets.

2. **Meaning of critical data storage or processing asset - section 12(F)**

   Many cloud infrastructure providers are open to public signup and any underlying customers.

   Vault submits that there should be a positive obligation on a data storage or processing provider (similar to the KYC rules and AUSTRAC reporting obligations of the banking sector) to make certain mandatory enquiries about their end users and workloads.

   For example, whether there will be (i) Government or critical infrastructure assets that use the provider's services or facilities, and (ii) for workloads of critical infrastructure assets, any 'business critical data' included.

   Community cloud models such as Vault's natively embeds these controls as part of a signup and workload classification process. As a result of this 'security by design' approach, Vault from the outset has been able to provide its cloud services at hyperscale and rates competitive with public cloud models that do not have these security controls.

3. **Meaning of cyber security incident - sections 12M, 30BD**

   Consider including the concept that an intended change in the ownership or control of particular stakeholders, such as a responsible entity for a critical data storage and processing asset, may of itself constitute a notifiable cyber security incident.

4. **Critical infrastructure risk management program - section 30AH**

   For critical data storage and processing assets, Vault recommends that the rules prescribe a minimum set of specific risks that must be addressed by the responsible entities of end users in their written critical infrastructure risk management program, as well as a mandatory set of mitigation steps for such risks.

   We submit that these include identifying the use of non-sovereign operational staff, locations and jurisdictions for critical data storage and processing assets as material risks, and what the associated mandatory mitigation steps are.

   For example, a mandatory mitigation step may be that 'PROTECTED' Government end user workloads, or critical infrastructure end user workloads that include 'business critical data', may only be with a fully sovereign data storage or processing provider that complies with the ASD's Essential 8 and is assessed under the Australian Cyber Security Centre's IRAP.

   Vault recommends mature and sovereign Australian standards and controls such as those of the Attorney General's Protective Security Policy Framework and the ASD's Information Security Manual, among other reasons, to further build sovereign capability for cyber security.