OFFICIAL

Mr. Andrew Hastie MP, Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

1 July 2019

Regarding: Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Dear Chair,

Thank you for the opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the amendments made by the Telecommunications and other Amendment (Assistance and Access) Act 2018 (AA Act).

Vault recognises that the reviews effectuated by the PJCIS are paramount in driving change, and as an industry representative impacted by the stipulations currently in place, would like to provide grassroot recommendations to encourage a wider scope perspective is encapsulated.

Vault gives consent for this submission to be published.

Vault Cloud

Vault is an Australian ASD/ACSC certified cloud service provider that operates the country's largest secure, sovereign, hyperscale community cloud for government and critical infrastructure. Vault's cloud infrastructure includes highly secure data centres to provide consistent, fast and scalable performance so that our clients can focus on their core business and scale from development to production rapidly without worrying about security, performance, reliability or capacity.

Vault takes securing the nation's data and privacy seriously and operates entirely within the legal jurisdiction of Australia and data held is not subject to the laws of a foreign country.

Vault is a trusted cloud provider to some of Australia's most sensitive data and mission critical systems. We have a proven track record in working with major Government agencies to move to the cloud as part of their digital transformation journey.

Economic Impact to Australia of the Assistance and Access (AA) Act

Media and public understanding of the AA Act have not displayed consistency with the AA Act itself. This public perception of the AA Act is having the largest economic impact to Australia.

Broadly this economic impact can be categorised in to two areas:

- export market economic impact; and
- domestic market economic impact.

Vault's Export Market Economic Impact

For commercial and confidentiality reasons we are unable to disclose details, but we can verify that the export of Vault's technology has been materially and detrimentally impacted by perception of the AA Act. As foreign governments and customers are assessing against a "media headline test", we are in an unfortunate position where logical persuasion is not sufficient to counter perception.

Domestic Market Economic Impact

Australia relies on the intellectual property of many multinational business. Vault, in turn, relies on technology, systems and software from many multinationals in the Vault Marketplace. These multinationals rely on Vault to provide hosting for their systems that are:

- Physically sovereign - data located on Australia soil
- Operationally sovereign - access to data is from within Australian; and
- Legally sovereign - data that is subject to Australian Law.

We are currently seeing **an exodus of data from Australia** including physical, operational and legal sovereignty.

The basis on which we have seen organisations make these decisions are broadly:

- Size of market; and
- perceived compliance burden of the jurisdiction.

Given Australia's comparatively small market size, we have seen multinationals "blacklist" Australia as a place to store data and, in some cases, that same company continues operations in China and Russia.

When multinationals choose to reduce or remove physical, operational and legal sovereignty from Australia the economic activity that supports these systems is also displaced, this results in a loss of:

- Australian jobs;
- growth opportunity; and
- taxation revenue.

Data Sovereignty Impact

Data sovereignty is a critical national security and privacy issue growing in complexity.

Sovereignty of data, access and control is something that Australians demand; the 2017 Privacy Commissioner's survey showed 93% of Australians expect data sovereignty and privacy is of paramount concern.

Mandating Australian cloud infrastructure sovereignty requirements is an important step in safeguarding overseas countries accessing sensitive government information. Unless a Government Cloud is fully Australian owned and operated it can be subject to the laws of other countries opening Australia up to cyber-terrorism and extreme security threat opportunities.

The DTA released a whole-of-government Hosting Strategy expedited sovereign assurance for data centre facilities, however technology platforms (where the data is held) such as clouds are not assured.

Recommendation 1: Expanding the sovereignty measures from the existing whole-of-government Hosting Strategy to cloud under a new "Data Sovereignty Policy". The government should mandate that all sensitive data hosted in cloud environments be sovereign (including legal data sovereignty), and that staff go through an Australian Government Security Vetting Agency (AGSVA) clearance where appropriate.

The government spends $47 billion a year through procurement and should prioritise economically grounded opportunities to deliver greater Australian resourcing capability, sustainability and growth.

Recommendation 2: Government Procurement Rules favour job creation, data protection, seeking to put Australia first and prioritising the benefits to Australia overall. Procuring agencies should be obliged to report on the value, separately to price, for contracts they have awarded based on this criterion.

Vault wants to see Australia keeping pace with global trends about privacy, sovereignty of data and ICT Procurement.

Access and Assistance (AA) Act Loophole

The AA Act addresses many law enforcement concerns that impact the security and safety of Australians, however the AA Act's perception detracts from the attractiveness of hosting data in Australia.

As multinational companies move physical, operational and legal jurisdiction offshore, they easily side step the AA Act - in effect thwarting the AA Act. Current legislation does not prevent these companies continuing to provide services to Australia citizens, companies or Government. In effect, these companies are eluding the law and attaining revenue while every day Australian citizens are suffering the consequences.

Recommendation 3: The Government urgently pass legislation that sets out clear data sovereignty requirements. In the absence of legislation, we recommend that the Government urgently issues policy that protects sensitive Government data such as health, social security and national security.

We understand that these issues are complex and welcome the opportunity to discuss them if further detail.

Mr Rupert Taylor-Price

[redacted]

Chief Executive Officer
Vault Cloud