Submission No 9

INQUIRY INTO CYBERSECURITY

Organisation: Vault Cloud

Date Received: 16 September 2020

Portfolio Committee No.1 - Premier and Finance,
Legislative Council,
Parliament of New South Wales,
Delivered by upload,
https://www.parliament.nsw.gov.au/committees/inquiries/Pages/lodge-a-submission.aspx?pk=2611

16 September 2020

Regarding: Submission to the Enquiry into Cybersecurity

Dear Committee,

Introduction 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 is a first for an Australian company. This agreement continues to cement the already established relationship with NSW Government agencies since 2018.

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.

Terms of Reference

1. That Portfolio Committee 1 – Premier and Finance inquire into and report on cybersecurity and digital information management in New South Wales, and in particular:

   (a) The number of cybersecurity incidents and data breaches involving NSW Government agencies;

   We are unable to answer the question to the specificity of a number as we are not clear on the definition of a cybersecurity incident. A data spill of sensitive data to the open internet or the dark web is a clear incident, however many incidents are far more nuanced. We are aware of a number of incidents (across many Australian Governments) where it is less clear if the incident has been recorded as such. Examples of this include:

   - Citizen data stored in a foreign owned cloud with extrajudicial control. Quoting from the ACSC website: "Foreign-owned CSPs, including those located in Australia, present additional risks that need to be considered as part of the overall risk posture. This includes foreign ownership, foreign interference and extrajudicial control over the CSP's operations and data holdings". Given the secretive nature of foreign surveillance programs (particularly in America, China and Russia) it is not possible to determine the severity of a breach when citizen data is held on a foreign owned cloud service. As such we would consider the hosting of citizen data on a foreign owned cloud an incident in and of itself. This issue is exacerbated when the Government stores the decryption keys in the same foreign owned cloud as the encrypted data.
   - Citizen data stored in a foreign owned cloud where data has been moved off-shore. We are aware of a number of incidents where citizen data has been moved offshore both by the cloud operator or by the cloud service provider. We would consider citizen data being moved offshore without citizen consent an incident.
   - Use of citizen data without informed consent. Some cloud service providers have business models where the data they hold is a monitised asset while at the same time providing a fee-for-service offering to host Government data. How citizen data is used in some of these cases, particularly in relation to metadata, is opaque. It is hard to determine at what point an incident has occured. There is a great deal of concern from citizens about how their data is being secured and used. This is evident from the Federal Government's announcements of "Sovereign Data Sets".

(b) The monitoring and response to cybersecurity incidents and data breaches across the NSW Government;

Substandard, or lack of, monitoring of cybersecurity incidents adversely impact effective responses to such incidents. Vault submits that monitoring must occur by solutions that meet certain objective standards of security, is the starting point for effective incident responses, and must be backed up by security certified or assessed incident response policies, procedures, plans and personnel.

Regarding monitoring solutions, the Federal Government has significant investment and experience in their Secure Internet Gateway (*SIG*) and Cross Domain Gateway (*CDG*) programs. A SIG is an Australian Signals Directorate (ASD) certified service provided both by Government agencies and the private sector that meets a standard set of security controls. SIGs are a perimeter protection hardware and software solution that help to detect cybersecurity incidents as well as prevent them in real time. This is a mature sector currently mandated to all Federal Government agencies. There is an opportunity for the NSW Government to leverage the pre existing investment made by the Federal Government.

It is an industry wide position that customers' connections to the Internet pose the majority of cybersecurity risks. In our experience SIGs and CDGs prevent or detect the majority of cybersecurity incidents when configured correctly and when there is secure management of their configuration.

Analysis of major data compromises has shown that a large portion of them occurred because bad actors within the organisation enabled the cybersecurity threat posed by the Internet. For this reason, to further enhance security, Vault locates its SIG solutions in Australia, and manages its SIG services for a customer by only accepting configuration instructions from a contractually pre-identified customer authorised individual. A further layer of security is added in that this individual cannot configure their SIG directly, and can only do so through a Vault staff member with the appropriate Australian Government Security Vetting Agency (*AGSVA*) clearance level.

Certified or security assessed SIGs and CDGs are also good monitoring solutions because they generate logs of all traffic that flow through them. These logs may be useful as a primary data source for cybersecurity incident reporting.

It should be considered whether the customers' Encryption Key Management or Tokenisation systems may be stored by the same organisation that provides Platform as a Service or Software as a Service to the customers. We are of the view that these systems should be separated and stored with a sovereign Cloud service provider on

behalf of the customer.

We respectfully submit that for purposes of enhanced cybersecurity, Digital Borders and Sovereign Data Control (including controlling cross-border data flows), the above principles should be legislated and become prescriptions under acts and regulations.

(c) The policies and procedures underpinning the management of digital information by the NSW Government;

The lack of harmonisation between State and Federal Government standards causes increased investment and reduced security. The Federal Government has invested significantly in both data classification and standards such as the ASDs Information Security Manual (*ISM*) and the Cth Attorney General's Protective Security Policy Framework (*PSPF*).

The national security lead data classification system (OFFICIAL, OFFICIAL:Sensitive, PROTECTED, SECRET and TOP SECRET) is widely used across Federal and international governments. A large ecosystem with "government grade" security already exists that applies the appropriate grade of security to a data classification. The lack of harmonisation on data classification also causes increased and sometimes duplicated investment.

Adopting the AGSVA security clearance process for personnel would also increase the ability to share secure information, systems, and personnel between Australian Governments. Vault has experienced situations where NSW Government employees were unable to access secure systems as they were designed around Federal Government security policies.

NSW Government might also consider supporting a Federal regulator for the data centre and Cloud services industries, and more specifically as it pertains to Government and Critical Infrastructure workloads (analogous to APRA for the Financial services industry). The regulator, apart from performing the functions of a regulator regarding the prescriptions mentioned, for example, can establish industry forums to further develop and roll out industry regulation.

It is not sufficient in our opinion for such a regulator's remit to only focus on data centres, because many of them merely act as physically secure location providers for Cloud service providers. The remit should also include Cloud infrastructure, platform and software service providers (referred to in the industry as Cloud IaaS, PaaS and SaaS).

(d) Systems management within NSW Government agencies including outages, backups and cyber security;

We recommend that NSW Government agencies avail themselves of the existing and tested sovereign capabilities of the Federal data classification system, IRAP and AGSVA clearance services, for the management of their systems to address cybersecurity risks, and use ISM and IRAP assessed data centre and Cloud service providers, to manage outages and backups.

(e) The financial costs and other impacts of cybersecurity incidents, data breaches and outages involving NSW Government agencies;

The challenge we see with the impact of a cybersecurity incident for the Government is in part the shared risk between all Government agencies. If a citizen does not trust an agency, their willingness to trust manifests in a singular view of Government. If the Department of Customer Service has an incident then citizens reduce their trust in the Department of Health. When citizens reduce their trust in Government agencies the Government s ability to service that citizen reduces.

Millions of Australians decided to opt out of eHealth primarily due to concerns about privacy, security and sovereignty. Opting out of eHealth results in diminished health outcomes including loss of life. The adoption of the COVIDSafe app was impacted due to the mainstream media coverage of the security concerns from using an overseas Cloud service provider instead of a sovereign provider. The Information Commissioner has stated that 93% of Australians do not want to see their data going offshore as early as 2017, yet we have not seen any NSW legislation that regulates data sovereignty.

Whilst we appreciate the political sensitivity of having strong border controls for Australia, most Australians appear to support this on the basis that Australia should have sovereign control over who comes to its landmass. Vault respectfully submits that the concepts of Digital Borders and Sovereign Data Control are analogous, go hand in hand, and may play a significant role in the level of trust that can be garnered from citizens for online Government services. In our view, by adopting the measures mentioned for Government services to citizens and perhaps even allowing for a public consultation or notice period for the placement of the citizen data and services, their trust will be significantly improved.

We are therefore of the view that the financial costs should not only be calculated as the costs to remedy the impacts of cybersecurity incidents, data breaches and outages, but also include the medium to long term efficiency costs and economic impacts due to Governments not being able to adopt Cloud services as a result of

lack of citizen trust. As mentioned, in Vault's opinion using sovereign Cloud services is an essential part of avoiding such costs and loss of life.

Vault is also concerned over the existence of a 'cultural myth' within Government Procurement agencies that hyperscale, high performance and high availability Cloud services are only available from overseas entities at competitive prices, and not from sovereign Cloud service providers. This is another reason why Vault is supportive of legally binding prescriptions to address the issues, which have the risk of being exacerbated should the prescriptions not be adopted at this time.

(f) Expenditure on cybersecurity, digital services and digital infrastructure across the NSW Government;

Vault recommends the following procurement targets for NSW Government to enable a sustainable and growing sovereign capability for cybersecurity, digital services and digital infrastructure:

- Target of 25% sovereign requirement in cybersecurity related procurements as well as the security components of tech procurements, with a commitment to grow this year on year as industry grows.
- This target would sit within a recommended overall 25% sovereign procurement target across the NSW Government.
- Determine Sovereign Data Sets that must remain within Australian jurisdiction (inline with the Federal Government)

(g) The management of public access to digital information under GIPA and similar processes including coverage of mobile based and online platforms;

By mandating the use of sovereign data centres and sovereign Cloud services for the hosting and storage of classified information, the NSW Government retains full control over such information including the management of public access to it under the *Government Information (Public Access) Act 2009*. We might also note that using sovereign data centres and Cloud services is by no means an inhibitor of cross-border data flows, but rather provides the necessary sovereign control over such flows.

In our opinion, in line with the ACSC, hosting classified or sensitive information with non-sovereign entities (even if hosted in Australia) may compromise, or place administrative hurdles on, the NSW Government's control of such information.

(h) Contractual arrangements between the NSW Government and providers of digital services

and infrastructure, including:

(i) Provisions relating to cybersecurity generally; and

We respectfully submit that for the NSW Government to control its Digital Borders and have Sovereign Data Control, the adoption of international cybersecurity standards, and controls, when Australia already has made significant investment in and has a mature set of Federal cybersecurity standards, controls, policies and procedures for online services, would be unnecessary, disruptive and detrimental to the ongoing control commensurate with sovereignty. Vault is also of the view that the international cybersecurity standards and controls are not necessarily superior. For example, in our view the standards and controls of the ISM as assessed against the IRAP are more comprehensive and of a better qualitative standard than international cybersecurity standards, controls and certifications such as ISO27001.

For these reasons, Vault has as part of its customer contract templates a commitment and obligation to its customers to remain in continuous compliance with Federal cybersecurity controls, standards, policies and procedures as well as any State based ones. Vault recommends that these should be standard provisions for contracts with any digital services provider to Government or Critical Infrastructure.

We also propose a contractual right for the industry regulator proposed above to audit compliance with these contractual terms, both for whether they exist, and are complied with.

(ii) Reporting obligations and the monitoring of cybersecurity incidents;

As part of contractually agreeing to the Federal cybersecurity standards, controls, policies and procedures, Vault accepts all the monitoring and reporting obligations placed on it under that framework. In our opinion this is a world leading framework, and as mentioned, one that is mature and can easily be adopted by the NSW Government. Harmonising reporting obligations and the monitoring of cybersecurity incidents with the Federal Government will reduce costs for suppliers.

In addition to the Federal requirements we would recommend that suppliers in possession of Government data must:

- report exactly where Government data is housed including any replica copies or potential copies as part of a disaster recovery plan;
- maintain and open records to inspection of any networks that the Government data has transited;

- maintain and open records to inspection of any people or systems that access metadata that in any way relates to Government data including the purpose of use;
- provide names and addresses of any personnel who could under any circumstances access any Government data (as defined by the ACSC: Customer data, Account data, Metadata, Support and administrator data) regardless of encryption;
- allow a security cleared Government representative to inspect the cybersecurity controls that segregate and control the movement of data including reviewing source code; and
- provide privileged step-in rights to Government for systems that relate to the possession of Government data if there is a cybersecurity incident.

(i) The extent and impact of outsourcing of government information systems, including:

(i) Outsourcing to entities which are owned overseas;

This practice, apart from inhibiting the ability to grow sovereign capability, in itself is detrimental to the control of Digital Borders and having Sovereign Data Control. Some of the reasons for this are described below.

- The size and efficiency of an overseas entity's operations (referred to as 'hyperscale') are not a reflection of the strength of its cybersecurity postures and capabilities. More specifically, hyperscaling is not unique to them and can be procured from a number of sovereign providers at similar or better prices.
- Enabling cross-border data flows is not a unique capability for overseas entities, but rather in their case poses a risk of uncontrolled cross-border data flows of sovereign classified data.
- Investigating or auditing the multi-jurisdictional operations of the overseas entities and in particular their claimed cybersecurity postures and operational practices in each of these jurisdictions, might be impossible or is impractical to a large degree.
- The overseas entities adoption of sovereign cybersecurity and operational practices and Digital Borders and Sovereign Data Control on behalf of a customer (i) might be merely 'lip service' that cannot be tested for substance, and (ii) is fundamentally in conflict with their publicly stated business models including open Digital Borders and support for unregulated cross-border data flows.

Australia's experience in border protection controls have shown that it leads to a stronger and more secure and sustainable economy, and are not economic inhibitors. Similarly, Digital Borders and Sovereign Data Control are not economic inhibitors and will lead to a stronger and more secure and sustainable economy for Australia.

- Adopting the cybersecurity standards and controls of the foreign jurisdiction of the overseas entity, or international ones, takes them out of sovereign control and leaves them vulnerable to not meeting sovereign interests and necessities.
- The global nature of the overseas entities operations and commercial interests create multiple substantial conflicts of interests.
- Conflicting legislation or legislative 'red tape' apply to overseas entities absent 'treaties', or even when 'treaties' are adopted between Australia and their home countries. This may also lead to unknown or uncontrolled sovereign data disclosures.
- The NSW Parliament cannot provide NSW citizens assurances or control security, privacy or sovereignty outcomes when the NSW Government provides overseas companies with access to NSW citizen data. Specifically, even if bilateral agreements were put in place with other countries, it is inconceivable that the NSW parliament would have material (or any) control over the future legislation of other countries.
- Operational control of support services and support personnel may be non-sovereign.
- Ownership or control of metadata relating to classified information may be compromised.
- Beneficial terms and true 'partnerships' are difficult to attain when Australia is too reliant on foreign digital infrastructure, services or technology.
- The US Government intentionally will not host their systems on Australian providers, this is compounded by "America First". The US Australia Free Trade Agreement allows this on National Security grounds. If Australia does not apply the same standard for Australian's data that the US does for its citizens it will accelerate the existing significant trade deficit.
- If Australia fails to build material sovereign capability, we will be failing to contribute to the five-eyes partnership and will remain a dependent consumer.

(ii) The risks involved with outsourcing government information systems.

The material risks involved with outsourcing government information systems that in our opinion need to be considered when a decision to outsource government information systems is made, are both on the customer's side and the outsourced provider's side.

For customers it is whether they applied appropriate security classification and management policies and procedures to the workloads, including data, the subject of the information systems to be outsourced (*Workload Cybersecurity Classification*).

Depending on the Workload Cybersecurity Classification level, or whether it is substandard or altogether lacking, it may reduce or increase the risks associated with the outsourced provider's side. These risks include whether the outsourced provider:

- owes allegiance to Australia or a foreign government
- has common security and economic interests that support and benefit Australia
- is subject to conflicting or potentially conflicting foreign jurisdictional control over its legal entities, operations or personnel
- transmits, processes, hosts or stores classified or commercially sensitive information on digital infrastructure located outside the geographical boundaries of Australia or on Public Cloud infrastructure (as opposed to Cloud infrastructure with a regulated user base)
- complies with independently certified or assessed sovereign cybersecurity standards and controls, or are subject to foreign technologies, standards and controls outside of sovereign control, for example, regarding data classification and system inventory management, configuration management, data encryption and privileged access management
- can be effectively investigated or audited
- has the services infrastructure and technology available to it to take over the information system and manage it at the same or a higher standard, and, for example, has Cloud hyperscaling technologies and improved system performance for latency and availability (which we note is available from a number of sovereign, certified and assessed Cloud service providers and data centres at highly competitive prices, and is by no means a unique attribute of large overseas entities)

- creates financial and service efficiencies previously unrealised
- has an acceptable reputation and track record of delivery
- has a sophisticated service and technology ecosystem with other trusted providers that it can draw on
- is able to assure sustainability of supply including through third party support arrangements including financial guarantees, and customer step in rights
- will be detrimental to the growth of sovereign capability
- will tie the customer into using its technologies and services and make it difficult to adopt competing or complementary offerings
- has a track record of uncompetitive behaviour or lack of sensitivity to supporting sovereign SME industry programs
- is selected purely from a delivery risk or price perspective without taking account of the other risks mentioned above.

By the NSW Government investing more in sovereign capability, many of the risks mentioned above will become negligible in our view.

(j) The support provided by the NSW Government to local councils and other organisations in relation to cybersecurity;

Not answered.

(k) The NSW Government's response to cybercrime in the community generally; and

Not answered.

(l) Any other related matter.

Not answered.

Yours sincerely,

Rupert Taylor-Price
CEO - Vault Systems Pty Ltd