

The Department of Home Affairs,  
Australian Government,  
Delivered by Upload to

<https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems/submission-form>,

16 September 2020

## **Regarding: Response to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper**

Dear Sir/Madam,

Please see below the responses of Vault to the majority of the questions posed in the Consultation Paper, which we hope will add value to the consultation process.

For ease of reference we have copied immediately below the industry sectors that the Department is targeting from a Critical Infrastructure (CI) perspective.

- + Banking and finance
- + Communications
- + Data and the Cloud
- + Defence industry
- + Education, research and innovation
- + Energy
- + Food and grocery
- + Health
- + Space
- + Transport
- + Water

### **Questions and Vault responses**

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

Vault operates two dedicated, air gapped, CI Clouds. We use the Home Affairs CI sectors as the guide as to who is eligible to use those Community clouds. As such we have many requests from industry and the only group that we felt compelled to service that was not covered were major Australian political parties. From our assessment a political party was

neither CI or Government but we deemed it vital to Australia's economy, security and sovereignty. Legal firms that are working on cases of national significance are another area where it is not clear if they are CI.

We have not experienced any other situations where something was vital to Australia's economy, security and sovereignty but not part of the Home Affairs CI sectors.

2. Do you think current definition of Critical Infrastructure is still fit for purpose?

Yes, but Vault believes that expanding it to include 'democratic wellbeing' will strengthen Australia's social and economic wellbeing, and security.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

Yes. Vault submits that entities that can in a material way affect Australia's free, open and democratic standards, should be prioritised as critical entities.

4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

Foreign, criminal or unlawful control or disruption of Cloud infrastructure, services provided over Cloud infrastructure, service personnel for Cloud infrastructure, and data hosted on Cloud infrastructure.

However we would like to answer the question in relation to the threats our nation faces rather than businesses. The sum of all business risks are not equal to the aggregate risk for Australia.

In another Home Affairs CI sector, Australia is very fortunate that its four largest banks are Australian. If the banking sector had formed in recent years it is conceivable that Australian major banks would be foreign owned and this would present an unacceptable aggregate risk to Australia. In the Data and the Cloud sector, unfortunately Australia is in the situation where the majority market share has gone to foreign companies.

In the Data and the Cloud sector we face a grave existential risk because:

- Cloud is rapidly expanding in all CI and Government supply chains; and
- Cloud providers operating in Australia are predominantly foreign owned, which according to the ACSC poses a [foreign interference](#) risk.

The majority market share of the Data and the Cloud sector has gone to foreign companies in part because:

- ASD formally [certified non compliant foreign owned Clouds](#) while at the same time enforcing compliance on Australian providers resulting in Australian companies operating at a disadvantage; and

- the Cth Government has put in place Whole-of-Government agreements with several foreign companies but no Australian companies.

According to the [AFR](#), “AWS, Azure, Google Cloud, IBM, Oracle and Alibaba Cloud – combined to make up around 82 per cent of local Cloud IaaS spending, with the first two well out in front.”

The result is an enormous aggregation risk, a black swan event beyond any Australia has seen. Conceivably, within a few years from now more than 51% of CI entities could have a critical supply chain risk on two foreign owned Clouds. For the avoidance of doubt, this could mean that the majority of Australia's CI could have a simultaneous outage including all the major banks, Federal and State Governments, Home Affairs CIC itself, communications, transport, Defence, defence industry and utilities. To compound this many PaaS and SaaS providers also leverage the IaaS of these Cloud providers often without the knowledge of the CI buyer - resulting in many auxiliary and support systems being down at the same time.

In 2020 both Google and IBM had global outages in all regions that lasted over 4 hours. We respectfully put forward that this aggregate risk is one of the greatest risks that Australia could face in the next decade in the absence of regulation.

**We have deep concerns that the Data and the Cloud sector has no regulator** while being the most critical CI sector as it links to all other CI sectors. The decades that APRA has taken to mature is not available in the Data and the Cloud sector.

The Data and the Cloud sector is also critical from a citizen trust perspective.

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 are only recently seeing requirements form for “sovereign data sets”.

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.

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.

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

With reference to the highest levels of interdependence, consequences of compromise and impact on maintaining open, free and democratic societies while ensuring Australia's economy, security and sovereignty.

6. Which entities would you expect to be owners and operators of systems of national significance?

Government and sovereign private commercial entities

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

Vault submits that the network and strategy need strong focus on aggregation risk. Vault recommends that no more than 25% of CI providers in a single sector should have supply chain dependencies from any single foreign country.

8. What might this new TISN model look like, and what entities should be included?

Not answered

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Vault submits that Government should have a specific focus on the information technology infrastructure environment of CI entities.

Government can support such entities by adopting clear and binding requirements for their information technology infrastructure environments, and more specifically the data centres and Cloud infrastructure that underpin it.

We propose that the requirements should focus on Sovereignty of the data centre and Cloud infrastructure supply chain and its ability to protect Digital Borders. For example, Vault is of the view that the Commonwealth Whole of Government Hosting Strategy may be strengthened further to take account of the above and made equally applicable to regulated and systems of national significance CI.

Specific standards set for this supply chain should consequently be built on local sovereign standards that are technology neutral (with a preference for open standards technology), such as Australian Standards and those of the Information Security Manual (*ISM*) of the Department of Defence and assessed under their Information Security Registered

Assessors Program (*IRAP*). As an analogy, Australian Standards have been highly effective in the Australian construction industry, and may play a similar role in the Australian Data and Cloud sector.

Government can further support such entities by establishing a regulator (akin to Financial Services regulators such as APRA) for the Data and Cloud sector supply chain. This may start off with the Home Affairs CIC that acts as an interim regulator, and transitions to an independent sector specific regulator established and governed by a Commonwealth law. For example, the law might be called the *Australian Data Centre and Cloud Services Regulation Authority Act 2021*.

The regulator should have investigatory, audit and step in powers, with the latter enabling it to itself or through a specialist third party take over affected operations of a critical data centre or Cloud asset for the CI entity.

10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Vault submits that further expansion is required on:

- sector aggregation risk;
- a clear regulatory authority for the Data and the Cloud sector; and
- specific sovereignty requirements.

11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

Vault submits that the security requirements do not meet the national security, security, economic and sovereignty risks that are present. Vault proposes that critical parts of CI should operate at no less than full compliance to the PROTECTED requirements of the ISM and the Attorney General's Protective Security Policy Framework (*PSPF*) while having physical, operational and legal sovereignty. Vault further proposes that critical parts of CI that pose a loss of life safety risk should operate at no less than full compliance to the SECRET requirements of the ISM and the PSPF.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Vault has invested in exceeding the principles outlined as Vault already operates a CI Cloud. Vault made this investment as the business case showed that the cost of not meeting a high security standard would be too costly in direct and consequential costs in the otherwise inevitable event of an incident. Vault works with an ecosystem of organisations that operate within the principles, particularly resulting from a level of regulation available today across Banking and Energy sectors, and whilst in other industries there will likely be an investment and longer time scale required to meet new security standards, Vault understands that these organisations would accept the necessity of the investment in

supporting secure Brand and ecosystem opportunity benefits. It is worth noting that in larger enterprise organisations (ASX Top 100), most will start from a relatively strong security governance position that will reduce impact beyond procedural adjustments, the greatest time challenge will lie in Australian headquartered multinationals and working through the alignment of global data jurisdiction requirements.

13. What costs would organisations take on to meet these new obligations?

The new obligations will set clear expectations and result in reduced costs for sovereign providers. An unregulated or poorly regulated Data and the Cloud sector is more costly as the domestic providers have to attempt to meet a number of non-mandated standards and second guess future investments. Costs would however increase for foreign owned providers as they would likely have to comply with their domestic regulator in addition to the Australian requirements. In other words the lack of these new obligations in the current market is increasing operational costs for some providers as there is investment uncertainty. These 'contingency' costs inevitably will be passed on to CI customers.

Whether potentially higher regulatory costs for some providers resulting from the new obligations for the Data and the Cloud sector will have to be borne by the CI customers, will depend on the arrangements in place with the providers. In Vault's case we from the outset had accepted the investment and expenditure associated with provisioning Cloud services at the IRAP assessed PROTECTED and SECRET level in accordance with the ISM and PSPF. Despite doing so, Vault's pricing to the market was and continues to remain competitive with Cloud service providers that do not meet these obligations. As mentioned, we have been of the view that the obligations will in fact lead to a stronger economy, security and sovereignty for Australia.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

A large number of the Data and the Cloud sector providers deliver services to the Federal Government which have similar and more onerous requirements. The investment reduces the costs as the cost of compliance is less than the cost of incident remediation and loss of reputation. Vault's indicative security, compliance and sovereignty costs compared to a China based provider are:

- Physical: 20% of all costs (Leases, power, infrastructure etc)
- Operational: 40% of costs (Audit, Australian wages etc)
- Legal: 15% of all costs (Cost of capital, tax etc)

Totalling 75% of all costs is significant, however as these costs are already incurred to service the State and Federal Government, there is 0% incremental cost for servicing CI. The risk born by not meeting these requirements would likely cost more than 100% of current costs.

Industry sectors that align to well formed security obligations today, albeit not completely aligned with the proposed CI obligations, are the Banking and Finance and Energy sectors. These sectors have aligned to regulatory frameworks influenced by bespoke research at the time, but not standardised at a National level. The result being enhancements in both reporting consistency and standardisation of security application will be required across these sectors.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

Increased clarity on requirements and obligations would reduce the need for providers to make speculative investments that may be superfluous. The lack of regulation in the Data and the Cloud sector results in security investments being undermined for organisations that want to “do the right thing” and results in brand being a stronger driver to buyer behaviour than tangible security.

Vault suggests that through introducing a Data and the Cloud sector regulator existing sector regulators could refine their focus, purpose and investment toward their speciality.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

Vault requests that clear sovereignty requirements be communicated based on the following structure:

1. Legal - the data is subject solely to the laws of the country of data origin. Generally this means that the custodian must be owned and operated within country.
2. Operational - data, metadata, monitoring and remote access are managed solely within the country of the data's origin.
3. Physical - the data at rest and in transit remains within the originating country.

Vault also requests that the data classifications used by the Federal Government be introduced to CI sectors to drive a simplified, common understanding and language for required obligations.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

Please see 9 above.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

Education sessions for all CI sectors on the use of Data and the Cloud including understanding aggregation risk and foreign interference in line with [ACSC guidance on Sovereignty](#).

19. How can Government better support critical infrastructure in managing their security risks?

By providing binding regulations that are clear on what the minimum requirements are for regulated CI and systems of national significance to be compliant with their PSOs. For example, by mandating the security assessment and sovereignty standards for their information technology environment supply chain.

The CIC could also provide information and education sessions to CI Boards to enable them to better understand and manage risks.

20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

AusCheck results on individuals may be useful for CI outside of Data and the Cloud, however given the sensitive and critical nature of Data and the Cloud, Australian Government Security Vetting Agency clearances for all staff that work for the Data and the Cloud sector providing services to Government or other CI sectors, should be mandatory at an NV1 level.

21. Do you have any other comments you would like to make regarding the PSO?

Given the history of variable security in relation to the Data and the Cloud sector, Vault resubmits the importance of having a full regulator and that the Government addresses sovereignty and aggregate risk concerns.

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Vault submits that a full and proactive Data and the Cloud sector regulator is required to identify and remediate cyber vulnerabilities.

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

Between 2014 and 2019 Vault collaborated with ASD on a daily basis on a number of complex matters. Vault submits that a full regulator is required to work with Data and the Cloud sector providers on a daily basis.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?



Vault advocates that all Data and the Cloud sector providers are mandated to share all global threat intelligence data with the Australian Government. The cost for Vault to do so would be minimal.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

Government and CI entities should be mandated to use ASD Certified Secure Internet Gateways and Cross Domain Gateways as this approach has proven effective for the Federal Government.

Early detection of malicious activity is vital but is reactive by nature, meaning that network security improvements are implemented post event leaving an organisation exposed to a quadruple cost impact;

- cost of outage;
- cost of remediation;
- cost of improvement; and
- cost to reputation.

Critical networks need to begin to proactively search for vulnerabilities "beyond the wire" before an attack occurs. This is considered the best form of harm minimisation in network security.

26. What are the barriers to owners and operators acting on information alerts from Government?

None identified.

27. What information would you like to see included in playbooks? Are there any barriers to codeveloping playbooks with Government?

Information for other CI entities around Data and the Cloud CI sector providers such as:

- compliance to the ISM and PSPF;
- Secure Cloud Provisioning guides;
- Connectivity guides;
- Data residency and Sovereignty guides; and
- Types of CI Systems and Cloud Use guides.

28. What safeguards or assurances would you expect to see for information provided to Government?

For information to be handled with PROTECTED security controls with 100% compliance.

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

Similar to step-in provisions for APRA. The Government should be able to step in when it reasonably believes there is a National Security risk, to prevent loss of life, to ensure the sovereignty of Australia or at a Minister's direction. The Government should be able to take

full control of infrastructure, systems and staff. The Data and the Cloud sector provider should provide a full copy of all data including metadata on request. Data and the Cloud sector providers should have an obligation to segregate CI data from non-CI data to avoid any cross jurisdictional regulatory disputes.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

Under a predefined set of criteria the CIC or regulator should be able to declare an emergency. Without restriction, the Minister should be able to declare the emergency.

Given the nature of an emergency, Vault advises not to have a mandatory advisory process.

31. Who should oversee the Government's use of these powers?

The use of these powers should be limited to operations of the CI sector, and there should be protections against the use of Government accessing sensitive private citizen data. Access of sensitive citizen data should be overseen by the provisions in the Assistance and Access Act.

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

An attack on Australian CI should be treated the same regardless of the perpetrators location. Australia should support a rules based and values based system. Discriminatory behaviour against certain locations serves to antagonise perpetrators, resulting in increased risk for CI.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

Officers that act within the prescribed emergency framework should be exempt from civil or criminal action. At the same time, to garner and assure continued industry support, the prescribed framework should exempt Data and Cloud sector providers from liability resulting from actions taken in respect of their operations by the officers.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

See 31.

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

- The lack of clarity about physical, operational and legal sovereignty has resulted in reduced domestic investment for the Data and the Cloud sector. This is addressed

by the CIC providing guidance in line with the ACSC guidance (see [Cloud service provider locality and ownership](#)).

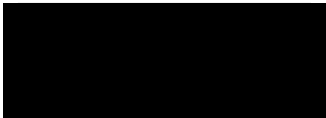
- CI buyers have difficulty ensuring sovereignty of their Data and the Cloud sector providers. There are concerns that a foreign investor could buy out a sovereign Data and the Cloud sector provider. This could be addressed by having an opt in binding commitment with the Government for a Data and the Cloud sector provider servicing regulated or systems of national significance CI, to remain sovereign, similar to the Commonwealth Whole of Government Hosting Strategy. Vault would be very keen on such a scheme and enter the binding arrangement - we understand that Canberra Data Centres has something similar in place with the Attorney General.
- The lack of a Data and the Cloud regulator has resulted in reduced investment due to lack of certainty. Appointing a regulator would address this.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

Vault considers the increased role of Government to be a factor in reducing risk and increasing certainty.

Please feel free to contact me with any questions anytime on [REDACTED].

Yours sincerely,



Rupert Taylor-Price  
CEO - Vault Systems Pty Ltd