Australian Government
Digital Transformation Agency

dta

Senate Economics References Committee

Inquiry into Influence of International Digital Platforms

Digital Transformation Agency (DTA) Submission

Introduction

This submission is intended to provide the Senate Economics References Committee with:

- Information to help inform the mapping exercise that is being undertaken, specifically to provide information on the regulation that is being conducted with some of the technology companies listed in the Issues Paper and other similar organisations.
- The Digital Transformation Agency (DTA) has limited its response to the questions in the Cloud Market section of the Issues Paper, as this is an area that it is currently undertaking regulatory activities.

Consultation Questions – The Cloud Market

Question 1: With respect to the cloud, what regulation that currently exists in other countries that could be of benefit to Australia?

The international regulation and legislation that may be relevant includes:

- Software Bill of Materials being developed by the United States
- The Network and Information Systems (NIS) Regulations 2018 in the United Kingdom
- Information Technology Security Act 2.0 in Germany.

Question 2: Should new assessments and oversight protocols for cloud computing products be implemented to bolster security of the cloud? If yes, how should cloud computing products be regulated?

The DTA currently assesses data centre and cloud services used by Australian Government customers to host information that is sensitive or classified up to 'PROTECTED' level under the Hosting Certification Framework (HCF). Service providers need to comply with a range of requirements that all data must be hosted with the appropriate level of privacy, sovereignty, and security controls. The HCF contractually binds (under deed) certified providers into maintaining controls for ownership, control, security, and data protection.

A list of providers that have been assessed and certified by the DTA is available on the Hosting Certification Framework website.[1]

The HCF is undergoing policy reform and one of the key consultation topics is the feasibility of expanding the scope to assess Software-as-a-Service, Managed Service Providers and System Integrators.

[1] Available at: https://www.hostingcertification.gov.au/certified-service-providers

More information on the HCF is provided in response to Questions 3, 4 and 5.

The DTA has whole-of-government arrangements with several large cloud providers often referred to as hyper-scalers. Current contract arrangements include Microsoft, Amazon Web Services, IBM, and Oracle. We leverage these agreements and the buying power of government to promote compliance with current policy and regulations.

Question 3: Would government regulation increase confidence in cloud services and provide greater clarity on accountability and have an impact on the benefits this technology?

Understanding that the Committee is exploring regulation to increase confidence of Australian citizens in cloud services, the DTA is assessing and certifying service providers that host government data that may include information on citizens.

The HCF ensures effective and consistent controls are in place for the Australian Government's critical systems and data holdings that are held by external hosting providers. In administering the HCF, the DTA seeks to address the rising use of online and digital services by Australians through increasing efforts to manage government systems and data holdings effectively and securely.

Question 4: What regulatory challenges are associated with the use of cloud services, particularly where data and information is stored in other jurisdictions? How might these regulatory challenges be addressed to ensure that consumers using cloud services are protected?

The DTA has found that global service providers, with workforces and facilities located outside of Australia, have had challenges in complying with some of the control objectives under the HCF.

Under the HCF, hosting providers are required to demonstrate that data will only move between customer and the agreed geo-locked strategic certified data centre facilities and will not leave Australia at any point.

An issue is ensuring personnel that would have unescorted physical or logical access to sensitive or classified government data, obtain Australian Government Security Vetting Agency (AGSVA) security clearances. There are also requirements around executive control and influence of strategic decisions that have been challenging for global providers.

The DTA is addressing these challenges in partnership with the relevant industry and government parties by applying interim controls to address the associated risks until the HCF requirements can be met. These issues are also feeding into policy consultation and reform activities under way.

Question 5: What can be done to promote competition in the cloud space rather than attempt some form of protection in this market?

The approach taken by the DTA has been to ensure a range of service providers for external cloud hosting are assessed and certified under the HCF to support market competition and meet government demand for services. It is not mandatory for service providers to register for certification. However, it is mandatory for Non-corporate Commonwealth Entities (NCEs) to use a service provider certified under the HCF to a 'strategic' level if they are being engaged to host sensitive or classified data.

On 29 July 2022, this was mandated in the Protective Security Policy Framework. To ensure service providers that have not yet been certified are not disadvantaged, NCEs can apply for an exemption for a specific hosting service contract in special circumstances.

Compliance with the Protective Security Policy Framework is backed by protections in our head agreements for our Cloud Marketplace and whole-of-government arrangements with big cloud providers, like Microsoft, Amazon Web Services, and IBM, who are also certified under the Hosting Certification Framework.

The Cloud Marketplace enables government to buy cloud products and services with assurance they are complying with relevant legislation and data security protections. Hosted with the DTA's other marketplaces and panels on BuyICT.gov.au, buyers can also easily search and identify cloud providers to include on requests for quotes, including small-to-medium enterprises (SMEs) and Indigenous-owned businesses. The guided workflows, utilised when approaching the market, prompt buyers to include multiple sellers, and to consider including SMEs and Indigenous-owned businesses.

If the Government wanted to further promote competition, it could consider:

- expand requirement to use a strategic-level Hosting Certification Framework-certified service provider beyond NCEs.
- introducing quotas or caps on the level of spend with a single provider or with the larger vendors.
- investing in local capability, including industry partnerships, seed funding, and linking on existing government initiatives
- providing guidance to agencies around breaking down larger cloud projects into smaller phases or deliverables that could be delivered by more than one provider.

Investing in local capability could grow the cloud industry in Australia, broadening the market and encouraging competition. Existing initiatives could be further developed and linked with other initiatives across government to uplift industry capability.

For example, the Commonwealth could consider adopting the Department of Defence's (Defence) initiative to develop Small the Medium Enterprise's (SME).

Defence's Office of Defence Industry Support (ODIS) works with State and Territory agencies, industry associates, and Defence's business partners, to help deliver capability to Defence. ODIS links with Australian SMEs to provide advisory, guidance and mentoring services and also offers industry grants valued from $15,000 to $1m, to support SMEs to meet the needs of Defence. You can read more about these measures here: https://www.defence.gov.au/business-industry/finding-opportunities/office-defence-industry-support/industry-grants

The Key Services of ODIS include:

- Specialist defence business advice, increasing the competitiveness of Australian Defence SME partners so they have the capability to integrate into supply chains and grow to become competitive providers.
- Direct linkages to Defence procurement programs through proactively identifying needs of Defence capability managers and delivery groups.
- Identify current SMEs who can meet Defence needs in the short term and assist to build the capability of Defence industry.
- Direct linkages to Defence end users to support innovative industry initiatives.
- Assist SMEs to work with end users, Defence projects and industry programs to support greater innovative industry outcomes.
- Tailor grants to assist the development of SMEs to meet Defence requirements in the short, medium and long terms.

This summary of the key services highlights that a dedicated approach is required to build growth in this sector.

DTA would recommend a similar initiative that links the Buy Australian Plan (led by the Department of Finance and the Department of Industry, Science, Energy and Resources) with the CSIRO's Data 61 and an office like ODIS to grow the cloud industry more broadly across Australia, rather than solely in the defence industry.

Finally, one of the impediments to cloud competition is the cost and complexity of the supporting management and reporting tools that have been developed by large providers over time. These are often proprietary in nature, and they are often critical in the cost-effective deployment of data and systems to the cloud. In most cases these tools are bundled with the cloud subscription costs and their use can create "lock-in" positions for their use.

One consideration to break this “lock-in” is the promotion of independent open source or third-party management and reporting solutions to be used. The use of these independent products can facilitate the use of multi-cloud (using more than one provider for the same workload) but also breaking the connection between bundled tools and the cloud service.