Ms Deborah Anton
Interim National Data Commissioner
Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

6 November 2020

Dear Ms Anton,

Exposure Draft – Data Availability and Transparency Act

Thank you for the opportunity to make a submission in respect of the Federal Government's exposure draft of the *Data Availability and Transparency Act*.

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit industry association and since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:
• providing a strong voice of influence;
• building a sense of community through events and education;
• enabling a network for collaboration and inspiration; and
• developing compelling tech policy thought leadership, government submissions and supporting state and federal government roundtables, committees and reviews.

We represent a large and diverse number of technology organisations in Australia, including:
• Multinational companies including all the major cloud platform providers and software vendors;
• National organisations including data centre owners, cloud providers, telecommunications companies and other tech leaders; and
• a diverse and large number of small and medium businesses, start-ups, universities and digital incubators.

Support for the scheme

The AIIA supports the ambitions of the *Data Availability and Transparency Act*. The secure release of data in the context of research and inter-agency exchange is desirable in the context of the open data principles to which the AIIA is committed. It should also well serve the aim of enacting 'Tell-Us-Once' principles across government services.

The clarity, simplicity and rigorousness of the scheme will be the watchwords for the effective implementation of the regime. Furthermore, confidence in preventing 'purpose creep' – whereby data is shared for purposes other than the named objectives of government services delivery, government policy development and research and development – will be essential to maintain public trust in the data sharing scheme.

Interoperability and capability

The Discussion paper stated (p.53):

> *Alongside work to progress the legislation, we are building the foundations and processes for transparent and accountable public sector data sharing. We are working with government agencies to develop effective systems to streamline requests for data and Data Sharing Agreements and searchable registers. We are also developing training and guidance to help government agencies apply the Data Sharing Principles. It will take time for the data system to mature and for Data Custodians and others to confidently use the new system.*

The Australian information industry is well-placed to support the government in its mission to make sovereign datasets interoperable and shareable. The development of effective, streamlined systems and registers, and the upskilling of the public sector, is a mission with which industry would be pleased to assist.

Privacy and security by design

The safeguarded privacy of the citizens to whom these reams of data relate is the major community concern. The AIIA believes that privacy and security need to be 'baked in' at the outset, just as the CovidSAFE app developed by the Federal Government in 2020 observed privacy-by-design principles.

End-to-end transparency and consent are important in this process; although the concept of implied consent has been discussed, the AIIA believes that consent to authorised data sharing should be made explicit at the citizen submission of data stage to maintain transparency and citizen engagement. This could involve each agency and each department embedding information about the DATA regime in privacy collection notices and forms.

De-identification concerns

Although privacy concerns have been somewhat allayed by the government's commitment to de-identification of data, past experience has shown that comparing data sets to identify individuals in secondary or roundabout methods is a concern. De-identification must not be a

process done hastily or assumed to be effective on its face; instead, rigorous 'white-hat hacking' should be undertaken by relevantly skilled public sector workers to ensure that identification is not possible by secondary means.

Impact on underlying infrastructure

By all accounts, it is participation in the dataset-sharing scheme that requires accreditation, but the way the legislation is worded in some places suggests that if a company is a service provider that holds or uses government data on the government's behalf that company also might have to get accredited. Confining accreditation to scheme participants needs to be made explicit in resulting legislation.

Another minor concern members have is the lack of definition in the Bill or the Explanatory Memorandum regarding the impact on underlying infrastructure (i.e. cloud).

The Accreditation Framework Discussion Paper page 10 says: "This does not impact on current data service provider arrangements (e.g. cloud infrastructure to host data assets). Other data services can continue to be contracted through standard procurement processes." However, the main Bill and Explanatory Memorandum do not include any similar statements.

It may be beneficial for the Bill to specify that where a scheme participant uses a service provider to hold and process data on the scheme participant's instructions, the scheme participant is not considered to be "sharing" the data with the service provider and the service provider does not need to participate in the scheme. This is necessary because:

1. The Bill does not define access or address use of service providers;
2. Service providers chosen to store data might not have expertise in data analytics and be ineligible to participate in the data transparency scheme. If scheme participants can only engage service providers who qualify to participate in the scheme themselves, scheme participants will have limited access to technology.

This is also important because service providers may not meet the ownership test set out in the legislation (see below).

Participation of 'Australian' organisations

The legislation states that Australian organisations are eligible for accreditation for participation in the scheme, and that companies seeking accreditation will be subject to an owesrhip test – which has not yet been specified – to confirm whether the ownership structure of that particular organisation or company meets an approved threshold. This needs to be defined and clarified.

Standards

As the AIIA has been invited to consider which existing arrangements should be formalised by the DATA legislation, we join with the Business Software Alliance in recommending that

the Australian Government adopt internationally-recognised cloud security certification standards.

Thank you for considering this response. Should you have any enquiries about the content of this submission, please contact policy@aiia.com.au.

Yours sincerely,

Simon Bush
GM Policy and Advocacy, AIIA