dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

info@dspanz.asn.au
**dspanz.asn.au**

14 May 2021

Critical Infrastructure Centre
Department of Home Affairs

Via email: ci.reforms@homeaffairs.gov.au

**Re: DSPANZ Response to Draft Critical Infrastructure Asset Definition Rules**

To whom it may concern:

Digital Service Providers Australia New Zealand (DSPANZ), formerly known as ABSIA, welcomes the opportunity to make this submission on behalf of our members and the business software industry.

We believe that many of our members will be affected by the legislation and asset definition rules as they:

- Provide services to entities likely to be classified as critical infrastructure assets;
- Operate in critical infrastructure sectors; and
- Transact sensitive tax and financial data.

Given the potential impacts on our members, DSPANZ would like to work with the Department of Home Affairs to minimise these impacts, where appropriate, and to ensure that the business software industry is supported through this process.

Other issues raised in the following pages of this submission include:

- The need for more information around how assets may be taken into and out of the critical infrastructure asset definition for a sector as threat landscapes evolve;
- Making more information available to assets and their ecosystems about liability, potential costs and proposed transition time frames; and
- Home Affairs should leverage existing industry practices to avoid excessive regulation.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese - maggie@dspanz.org.

Yours faithfully,

Simon Foster,
President & Director
DSPANZ

Formerly ABSIA

**About DSPANZ**

Digital Service Providers Australia New Zealand is the gateway for government into the dynamic, world class business software sector in Australia and New Zealand. Our members range from large, well-established companies through to new and nimble innovators who are working at the cutting edge of business software and app development on both sides of the Tasman.

**Potential to impact every and any business operating within a critical infrastructure sector**
Our members include software providers who provide services directly to entities that will be defined as critical infrastructure assets and others who will operate in the newly defined critical infrastructure sectors. They also include DSPs who transact sensitive tax, accounting, payroll, superannuation and financial data via APIs with government agencies and other service providers. These types of data transactions could easily see many of our members identified as critical data storage or processing assets under this definition in the critical infrastructure legislation.

Any organisation that operates within a designated critical infrastructure sector can be subject to ministerial intervention and therefore directed to perform actions, where necessary, to protect critical infrastructure assets even though the organisation itself may not have been designated as having critical infrastructure assets.

While these broad definitions will enable flexibility in determining what is and what is not a critical infrastructure asset as critical infrastructure sectors grow and threats evolve, the process in which assets will be defined as critical or not remains unclear. If Home Affairs is able to arbitrarily bring assets into or out of the asset definition for a certain sector, then it will be incredibly difficult for businesses to plan for or even assess the impact of any impending requirements. It is important to make these processes clear and set expectations on how this will be handled on an ongoing basis.

**Supporting critical infrastructure assets and their ecosystems**
For critical infrastructure assets to have confidence in how they will be regulated, they will need more information about the liability and potential costs involved if a cyber incident were to occur. This also extends to potential implications for the ecosystems of critical infrastructure assets. A first step could be making the processes transparent for the four sectors already designated. This allows for a better understanding of how new assets may be affected. Further, there should be processes in place for appealing decisions and reasonable notice periods.

For some assets, the critical infrastructure rules may be the first time they are being introduced to a regulatory environment or the first time they are being required to regulate their ecosystems. They will require additional time to adjust - and in some cases, they will need to raise capital or transform their operations.

To support all new assets coming under this regulation, Home Affairs will need to implement appropriate transition arrangements while companies determine, fund and implement actions to satisfy any new requirements. It is important to note that the cost of compliance could be significant and government financial assistance should be available to critical infrastructure assets to help cover costs and mitigate risks.

**Recognise existing processes and regimes**
Home Affairs have stated that they will look to leverage industry practices where effectiveness can be demonstrated. However, the degree to which they will be leveraged is currently unclear.

To better support our members, we recommend that Home Affairs recognises the below security standards and frameworks currently in use:

- GNGB - Gateway Services Standards for Gateway Operators transacting within the Superannuation Transaction Network
- GNGB - Annual incident response exercise
- ATO - Digital Service Provider Operational Framework
- DSPANZ - Security Standard for Add-on Marketplaces (SSAM)
- APRA - Prudential Standard CPS 234 Information Security

We would appreciate more information from Home Affairs about how these may be leveraged in meeting the Positive Security Obligation. DSPANZ can provide more information about each of these security standards mentioned above upon request.

DSPANZ wishes to emphasize that Home Affairs should avoid further fragmentation of cyber regulation and standards. Consideration should be given to a whole-of economy approach to regulating critical infrastructure sectors which includes regulating the assets as well as their ecosystems.