dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

C/- Hudson Gavin Martin
Level 16 45 Queen Street
Auckland 1010

hello@dspanz.org
dspanz.org

1 March 2024

Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Via online form.

Re: 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry.

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

DSPANZ broadly supports the measures raised in the consultation paper that will enable the government to share cyber security information with industry. We continue to advocate for threat intelligence sharing from government agencies, particularly the ATO, to help Digital Service Providers (DSPs) identify and mitigate potential threats and better understand the threat landscape.

In summary, DSPANZ provides feedback on the following measures:

- Further understanding cyber incidents - Ransomware reporting for businesses;
- Encouraging engagement during cyber incidents - Limited use obligation on the Australian Signals Directorate and National Cyber Security Coordinator;
- Learning lessons after cyber incidents - A Cyber Incident Review Board; and
- Protecting critical infrastructure - Data storage systems and business critical data.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese for more information.

Yours faithfully,

Matthew Prouse
President & Director
DSPANZ.

Belinda Stewart
Director & Security Committee Co-Chair
DSPANZ.

Measure 2: Further understanding cyber incidents - Ransomware reporting for businesses

8. What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?
A business's cyber security expertise and resources will impact its ability to meet this mandatory reporting requirement. The government should consider that it may be difficult for some businesses, especially smaller businesses, to provide detailed and timely information when determining the mandatory information required in reports.

9. What additional mandatory information should be reported if a payment is made?
The second report should avoid duplicating any information in the initial report to minimise the reporting burden on businesses.

10. Which entities should be subject to the mandatory ransomware reporting obligation?
Limiting the mandatory ransomware reporting obligation to larger businesses would avoid adding this compliance to smaller businesses that may not have the expertise or resources to meet the reporting obligation. While limiting the obligation would restrict the sample size, it would increase the information available to government and industry about ransomware incidents.

DSPANZ recognises there may be opportunities to expand the obligation to smaller businesses in the future. In the meantime, the government could encourage small businesses to report ransomware incidents voluntarily.

11. Should the scope of the ransomware reporting obligations be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?
As suggested above, limiting the reporting obligation to larger businesses would benefit smaller businesses, who may not have the expertise or resources to meet the reporting obligation.

While an annual turnover of more than $10 million per year may be an appropriate threshold, the government should consider how the ransomware reporting obligation would impact growing businesses and those that may fluctuate around the threshold each year.

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?
DSPANZ supports a 72-hour reporting timeframe for ransomware incidents to align the obligation with other mandatory reporting requirements, including the ATO's DSP Operational Security Framework.

DSPANZ recognises that shorter reporting timeframes may result in the government receiving lower quality data and information about incidents.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?

DSPANZ supports introducing no-fault and no-liability principles alongside ransomware reporting to protect entities.

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?
DSPANZ supports the government sharing ransomware reporting information with industry through public reports and other targeted communications.

DSPANZ would expect that most of the information shared with industry would be anonymised or aggregated unless there is an agreement between the government and a particular business to be identified in reports.

Measure 3: Encouraging engagement during cyber incidents - Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

Introducing a limited use obligation is a step in the right direction towards improving engagement with the ASD and Cyber Coordinator around cyber incidents.

DSPANZ recognises that organisations who are required to report cyber incidents outside of the ASD and Cyber Coordinator will not benefit from a limited use obligation. For example, the ATO cannot share cyber incident information back to organisations or individuals who may be involved or impacted by incidents due to tax secrecy provisions.

19. What else can government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?
As noted in the discussion paper, there are various reasons why the government may experience differing levels of engagement with industry around cyber incidents, such as being referred to legal representatives and delays in providing information. DSPANZ anticipates that some of these challenges may not necessarily change solely through introducing a limited use obligation. The government should work closely with industry to better understand these shared challenges and improve cyber incident reporting processes for all parties involved.

The government should play a role in reducing the compliance burden around mandatory cyber security reporting obligations. DSPANZ views creating a Digital Economy Regulator - a central source for security, certifications, data standards, and other requirements for market participants leveraging Commonwealth Government APIs and digital interactive sources - as a potential avenue to reduce this compliance burden.

Measure 4: Learning lessons after cyber incidents - A Cyber Incident Review Board

DSPANZ broadly supports establishing a Cyber Incident Review Board (CIRB) so long as it adopts a 'no-fault' approach when reviewing cyber incidents.

Measure 5: Protecting critical infrastructure - Data storage systems and business critical data

DSPANZ broadly supports changes to the SOCI Act to protect business critical data better. However, any changes should be a part of a larger economy-wide conversation on record-keeping and retaining data beyond minimum retention periods.

As a part of any work in this space, DSPANZ recognises there is an opportunity for the government to better define minimum and maximum data retention periods across current legislative requirements.