



Consultation on the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Submission by Deakin University

November 2020

Consultation of the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Submission by Deakin University, November 2020

Deakin University is pleased to contribute to consultation on the Exposure Draft of this Bill.

As can be seen from the detailed engagement by Deakin with the issues raised by the *Protecting Critical Infrastructure and Systems of National Significance* consultation process, Deakin is alive to the myriad of issues faced by the Commonwealth and the need for our nation to support and protect its critical infrastructure.

Since 2003, Deakin University has been a leader in cyber security research, education and innovation in Australia. Deakin has been awarded cyber security educator of the year for three consecutive years and has a range of undergraduate and postgraduate courses focused on cyber security, including combined undergraduate degrees with law and criminology. Deakin jointly with NTT (formally Dimension Data) supports Australia's only dedicated cyber security start-up accelerator, CyRise, now in its fourth year.

Deakin takes a holistic approach to cyber security, which includes Artificial Intelligence (AI), Information Technology (IT), data analytics, engineering, business and law, policy and regulation, psychology, humanities and health as these fields directly intersect with the future of our economy.

Deakin University is in the process of joining the Australian Technology Network group of universities (ATN) and fully supports the submission made by ATN in respect of this Bill.

It is with this background that Deakin makes these further short points in relation to the Bill.

Insufficient clarity

The Bill leaves much to be developed by Rules. Clear guidance in the Bill itself leads to certainty and transparency – critical for a positive approach to implementing the Bill's objectives.

Deakin submits that the Bill itself should be further developed and refined in order to produce a statute that is more nuanced and detailed in its application, and resulting in a reduction in the reliance on subsidiary legislation.

Reach

Deakin concurs with the premise set out in the Bill that Australian universities do hold and manage some nationally critical infrastructure assets. However, we do not agree that the entirety of a university's assets should therefore be classified as critical infrastructure assets. There are onerous operational requirements and significant fiscal penalties, if a university fails to meet the regulatory regime set out in the Bill for critical infrastructure. Such a regime should be tightly targeted to only those assets that are truly of national significance.

We submit that the Bill should specify a clear test and/or threshold to ensure that only those assets held or managed by a university that meet an objectively determined national critical infrastructure test should be within the scope of the Bill.

Inefficient Oversight

Universities are already subject to significant scrutiny by the Commonwealth – including but not limited to the following:

- primarily through TEQSA as the higher education regulator, and with oversight by the Minister for Education and Training
- by the Department of Defence (specifically in relation to Defence Trade Controls)
- by the Minister for Foreign Affairs and Trade (specifically in relation to Autonomous Sanctions and shortly in relation to Australia's Foreign Relations (State and Territory Arrangements) Act
- by the Attorney-General's Department in relation to the Foreign Influence Transparency Scheme Act.

Now it is proposed for Universities to also be subject to this Bill by the Department of Home Affairs.

Each of these organs of government has its own regulatory expectations and each regime requires resourcing by the University to meet the specific and differing reporting and other requirements.

Deakin submits that it is an additional and unfair regulatory burden to add to the existing compliance regimes. A simpler and more efficient approach may be to centralise and co-ordinate the Commonwealth's various national security requirements through one body that is tasked with liaising with universities.

In the alternative, Deakin submits that the Bill should recognise and address the costs of compliance with the regulatory regime imposed, which is currently unfunded

Deakin actively engages with agencies – Federal and State- in respect of cyber security concerns and measures to address those concerns. It will continue to do so. If the Commonwealth wishes to further regulate this activity, Deakin urges the Commonwealth to heed the matters raised by Deakin University, the ATN and Universities Australia in relation to this Bill to ensure the best outcome for the national security objectives of the government.