WESTERN SYDNEY
UNIVERSITY

27 November 2020

Western Sydney University submission to the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Western Sydney University welcomes the opportunity to respond to the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*.

We note that the Bill proposes to extend the Security of Critical Infrastructure (SOCI) Act 2018, to include new sectors of the Australian economy including higher education and research. Inclusion of universities under the SOCI Act imposes significant requirements of critical security infrastructure delivered through sector-specific measures, a risk management program, mandatory cyber incident reporting, and enhanced cybersecurity obligations for assets and systems of national significance.

Whilst acknowledging the critical importance of a secure higher education and research infrastructure, we emphasise that universities should be involved in co-creating the rules for a critical infrastructure risk management program that ensures universities are not unreasonably burdened with additional regulations and costs. The use of a coordinated, government- and sector-wide approach that takes into consideration existing structures and regulations such as the Defence Industry Security program, Defence Trade Controls Act 2012 and the Higher Education Integrity Unit within TEQSA to manage the University Foreign Interference Taskforce.

Where the legislation applies to the higher education and research sector, the requirements should be fit for purpose, and proportionate to the risk, using a targeted and coherent approach that does not impose an unreasonable financial and administrative burden on universities. Furthermore, the legislation should neither restrict academic freedom, a core foundational principle that has enabled the development of Australia's world-class higher education sector, nor unnecessarily degrade collaborations between universities and industry partners.

In addition to supporting University Foreign Interference Taskforce (UFIT) activity, the university sector is responding to increasing cybersecurity threats through the coordinated activities of the Australasian Higher Education Cybersecurity Service (AHECS). This work is led by CAUDIT in partnership with the universities, AARNet, AusCERT, Australian Access Federation (AAF) and the Research Education Advanced Network New Zealand (REANNZ). This network is working together to provide awareness-raising training, benchmarking, maturity assessments, coordinated threat intelligence and a sector-specific SOC provided by AARNet, amongst 11 workstreams in total. These actions will proactively help safeguard the intellectual property, digital assets, people, and hence reputation of Australasia's universities.

Nonetheless, for universities to meet their enhanced cybersecurity obligations that relate to systems of national significance, significant Government support is required. This will equip universities to be adequately prepared for, report, and respond to cybersecurity incidents. In addition, it is critical for the Government to provide disclosure protection that is currently non-existent. Finally, whole of sector training and resources for monitoring need to be developed by key government agencies to assist universities with their important work to protect critical infrastructure.

Recommendations

It is recommended that Government consider:

1. Using a broad, coordinated approach that takes into consideration currently existing relevant regulations and industry-based standards to avoid generating unnecessary regulatory burden on the higher education and research sector.
2. Ensuring that the legislative requirements are proportionate to the risk and apply a risk-based model that considers an institution's scale, complexity, capability and susceptibility to threat of critical infrastructure.
3. Incentivising universities to meet their cybersecurity obligations.
4. Providing disclosure protection that enables disclosure of protected information in the interests of national security.
5. Committing key government agencies to the development and provision of training and resources for use in protecting critical infrastructure.
6. Consulting more broadly with universities prior to introducing the *Security Legislation Amendment (Critical Infrastructure) Bill 2020,* to the Parliament.