Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Griffith Submission to the Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018.

Thank you for the opportunity to make a submission to Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018.

The submission is based on the Griffith submission to the Protecting Critical Infrastructure and Systems of National Significant Consultation.

Context of 2020

The impact of COVID-19 upon the University sector is unprecedented and unparalleled. The challenges and uncertainty have caused major disruptions to the University sector in 2020 and this uncertainty is set to continue in 2021 and beyond.

Griffith's risk and regulatory environment has increased in complexity over the last 12-24 months and this is set to continue over the coming years with the introduction of Australia's Foreign Relations (State and Territory Arrangements) Act 2020.

Griffith (and the sector) is addressing these challenges by redefining our University's shape, size and priorities to ensure we continue to achieve the University's mission given the constraints of significantly reduced income streams and increasing regulatory complexity. It is within this context that we submit this response.

Security of Critical Infrastructure

Griffith recognises the importance of uplifting the security and resilience of critical infrastructure. Furthermore, Griffith supports the principle of introducing safeguards to ensure disruption to the supply of essential services across Australia is minimised. Indeed, with respect to the cyber domain, Griffith and the sector more broadly has pivoted to improve protection against cyber threats.

Compliance with this legislation in its current form would require significant time and financial investment would be required. As a consequence, in our earlier submission, we advocated for a staggered implementation timeframe that seeks to maximise the regulatory platform of 'Government Assistance' (e.g. the Government work with AARNet to sponsor a national CTI (computer telephony integration) platform for the sector).

It is essential that assessment of the security of critical infrastructure remains proportionate to the risks presented; in this respect, we have concerns that the Bill does not adequately reflect the nuances of the Higher Education sector. We seek to understand in practicable terms and in greater detail the additional security obligations arising from the enhanced framework to the education, research and innovation sector. We have concerns of the *positive security obligations* on the sector. We understand

these obligations will carry significant reporting requirements, as well as requiring additional investments to meet expected standards in physical infrastructure, cyber infrastructure, personnel and supply chain.

We note that our internal processes focus on ensuring that we have fit-for-purpose governance and capabilities in order to appropriately and proportionately manage and mitigate inherent risks. By means of example, in response to Countering Foreign Interference Guidelines, we have established a Countering Foreign Interference Working Group which has undertaken a comprehensive review and assessment of risk areas across our activities with international collaborators. We have developed guidelines for reducing the risk of foreign interference to ensure that the local and national benefits of these relationships and collaborations can continue to be realised securely.

Recommendations

Universities around the country, including Griffith, face significant and ongoing economic challenges arising from the COVID-19 pandemic, and we are keen to focus the resources we have on the best possible outcomes for teaching, learning and research, while ensuring the protection of critical infrastructure and systems.

Griffith University outlines four recommendations that balance security requirements without imposing an unnecessary regulatory burden for consideration:

1. **Recommendation 1: Encourage collaboration**
   Further consultation and collaboration should be undertaken with the Higher Education sector to design a measured and proportionate framework which is focused on critical capabilities and assets. We advocate for greater collaboration with the sector to produce a unified cyber security strategy which would cover physical, people and cyber security issues; and bring together related compliance requirements such as University Foreign Interference Taskforce (UFIT) guidelines, Privacy Act Notifiable Data Breaches scheme, and the Security of Critical Infrastructure Act 2018 legislation.

2. **Recommendation 2 – Detailed consultation with sector cyber security subject matter experts**
   We propose further detailed consultation with the university sector including directly with the Australasian Higher Education Cyber Security group (AHECS) before introducing the amendments to the Security of Critical Infrastructure Act 2018. AHECS was specifically formed as a whole of sector initiative in response to growing cyber security threats to the higher education sector.

3. **Recommendation 3 – Narrow scope and staggered implementation timeframe**
   The proposed scope of the legislation, as applied to the Education, Research and Innovation sector for universities, should be narrowed to allow risk-based targeting of critical capabilities and assets. This would take into consideration the substantial investment required to implement existing recommendations outlined in UFIT guidelines and to increase the maturity of cyber security capabilities within the sector.

Griffith University
9 February 2021