WESTERN SYDNEY
UNIVERSITY

January 2022

Western Sydney University submission to the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 – Exposure Draft

---

Western Sydney University is strongly committed to working with the Commonwealth Government to prevent and mitigate the impact of cyber threats to critical infrastructure assets in the Higher Education Sector and Research. We welcome the opportunity to respond to the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* Exposure Draft (the *Bill*).

Western Sydney University acknowledges the importance of protecting Australia's critical infrastructure assets from cyber security threats, and in collaborating with the Commonwealth in building comprehensive defences against these threats both nationally and independently. We understand the value of the *Bill* and the Draft, as it provides a valuable guide in ensuring a robust response to cyber-intrusions, and a valuable reporting regime to assist both the Commonwealth and other critical infrastructure assets in responding to and identifying threats.

Our comments relate to three key areas of the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*:

1. Research Assets

It is understood that universities will need to report on cyber-intrusions or threats relating to specific research assets that have been identified and notified by the Secretary. To improve potential response times and ease the burden of reporting, Western Sydney University would appreciate further information relating to areas of research which are seen as being of 'national significance'. Alternatively, providing a narrowed draft list of research areas that could potentially be of national interest will allow universities to pre-empt potential reporting requirements, and ensure additional due diligence against relevant fields of research.

Given the current reporting obligations under the Foreign Arrangements Scheme, we would also recommend a review of the incident reporting process to coincide with information already captured through other Commonwealth reporting obligations.

2. Incident Response Planning & Cyber Security Exercises

It is understood that if requested by the Secretary via written notice, universities must undertake a cyber security exercise in relation to the system (of national significance), and all types of cyber security incidents, and do so within a predetermined time period.

Universities will need further guidance on what such an exercise must entail, as well as resources and templates to assist. While an asset has not been identified as having a 'system of national significance', it would also be beneficial for advice to be provided in terms of establishing a more robust Critical Incidents Response Plan, and for Commonwealth led training and information relating to cyber security exercises to ensure the sector remains on par with other critical assets.

3. Industry Specific Guidance & Consultation

Western Sydney University appreciates the effort provided by the Secretary of Home Affairs in informing and consulting with Australian industries and critical assets. However, the nature of the advice has been generalist and has led to some confusion throughout different sectors. We would request the opportunity for further Commonwealth guidance, particularly relating to the Higher Education and Research sector to fully understand our obligations under the *Bill*, and to ensure sector wide capacity to meet any reporting requirements.

As the Commonwealth continues to work closely with Western Sydney University, we appreciate the opportunity to identify areas for comment within the Exposure Draft and will continue to collaborate with both the Commonwealth and other critical assets to ensure both compliance and understanding of the *Bill*.