



Review of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and Statutory Review of the *Security of Critical Infrastructure Act 2018*

The Parliamentary Joint Committee on Intelligence and Security

IRU opening statement

The Innovative Research Universities welcomes the opportunity to engage with the Parliamentary Joint Committee on Intelligence and Security concerning the *Security of Critical Infrastructure Act 2018* (the Act) and proposed amendments to it.

Universities are a significant part of national infrastructure. Cybersecurity targets an area of great concern where the university commitment to openness and sharing of information to advance knowledge, runs against actors who would disrupt our operations. Disruption to our operations could cause significant harm if prolonged.

Universities are as keen as the Federal Government that their operations are not put at risk. IRU members are active in working with all advice, from Governments and others, to reduce risks and to act when incidents occur.

To date there have been no major incidents at an IRU member. We regard the experience of some other universities as an indicator of how close we may have been, not a sign to consider current actions sufficient.

The question is thus about what else is required, what continued long term cyber defence activities are needed – and whether the array of Government legislation against foreign interference, of which the Act is one, cohere as best they should to assist and protect universities.

The inclusion of higher education and research as a critical infrastructure sector (proposed section 8D) as part of the major expansion of the Act needs to be considered in this light. How do the provision of the Act if amended improve defence of universities against cyber attack? Are all the provisions required? How likely is it that the provisions of the Act as amended will be switched on for higher education and research?

There are many new powers in the Bill for the Government, supported by a complex array of plans, reporting and notifications, notably the critical infrastructure risk management program. IRU appreciates the work of the Critical Infrastructure Centre since the Bill was tabled to work up with each sector what the program should require and how to take account of existing arrangements. For universities the leading actor should be the Universities Foreign Interference Taskforce.

With an effective scheme of response worked out with the sector there should be little need to order actions or set up more administrative procedures. Instead, there would be effective joint action by university and security agencies to minimise adverse incidents involving Australia's universities.

6 July 2021

iru.edu.au