

# SUBMISSION TO THE PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE CONSULTATION

September 2020

Universities Australia (UA) welcomes the opportunity to make a submission to the *Protecting Critical Infrastructure and Systems of National Significance* consultation.

UA is the peak body for Australia's 39 comprehensive universities. Our members are spread across Australia, in both regional and metropolitan areas. They educate more than a million students each year and undertake research that both underpins and drives innovation in the economy.

Universities have a long history of working collaboratively and effectively with government agencies on security matters, such as the amendments to the Defence Trade Controls Act 2012 and, as partners in the University Foreign Interference Taskforce, to develop and implement *The Guidelines to counter foreign interference in the Australian university sector*. Australian universities recognise that they are a key element in ensuring Australia's prosperity, social cohesion and security.

This submission presents the key principles and issues in relation to the university sector, which is a part of the *Education, Research and Innovation* sector that was identified as one of the target sectors for inclusion in the amendments to the *Security of Critical Infrastructure Act 2018* (the Act). Our members appreciate the Commonwealth's invitation to work in partnership with the sector to develop proportionate requirements that maintain a careful balance between security and workability.

Universities Australia would be pleased, on behalf of its members, to work with the Department of Home Affairs further on the detailed and important work required to develop proportionate requirements through the identification of appropriate thresholds and scope.

## RECOMMENDATIONS

Universities Australia recommends that:

1. Government consult in greater detail with the university sector before introducing the amendments to the *Security of Critical Infrastructure Act 2018*;
2. the proposed scope of the legislation, as applied to the *Education, Research and Innovation* sector for universities be focussed to allow a proportionate, risk-based targeting of critical capabilities and assets; and
3. Government work with the university sector in developing an implementation timeframe that matches the maturity of the sector and takes into account the level of financial investment.

## KEY POINTS

### ***Consider focussing the scope and developing appropriate thresholds***

All universities are in scope as a 'regulated critical infrastructure entity' under proposed amendments to *Security of Critical Infrastructure Act 2018* (the Act).

This represents coverage of the university sector as a whole, an approach that has not been applied to any other sector in the economy.

Universities comprise a number of different types of businesses and activities, some of which may be appropriately recognised as critical infrastructure and some which would not (e.g. include sporting infrastructure, wildlife sanctuaries and so on).

If we take the Health sector as an example, one might wish to protect the delivery of emergency services however, that does not mean that all health providers need to be in scope. Even when included, only those meeting a particular threshold are truly critical to ensuring the health of Australian collectively.

The private sector undertakes the majority of R&D activity by total expenditure. All industry sectors undertake R&D, but it is largely concentrated in the professional, scientific and technical services; manufacturing; financial and insurance services; and mining sectors.

This Bill does not include those sectors as critical infrastructure entities. This would impose a significant, inappropriate burden. The same can be said for education (including vocational education, schools and non-university higher education providers).

The scope could be narrowed in a range of ways. Universities have a range of assets and capabilities that may be considered to be critical for the delivery of education services, for undertaking and collaborating on research and for the translation of ideas into products and services. Most of what may be termed critical assets are shared assets, underpinned by shared enabling infrastructure (such as supporting networks and authentication systems). Major research facilities and their enabling infrastructure are often shared assets between universities, industry and government partners.

The positive security obligations proposed for the sector are expected to require significant investments in new assets and training for the sector and for the companies that support the sector. Imposing an entity level obligation would be onerous, resource intensive and badly targeted.

Universities Australia does not agree that all higher education providers should be included and advocates for a more nuanced approach. Universities have demonstrated, through adapting to COVID-19, that many activities can continue despite major disruptions to Australia's normal way of life.

UA strongly supports the Government's stated approach that the legislated scheme will be proportionate to risk, and advocates for a targeted approach to assessing and managing risk in the higher education sector. Due to the broad range of university activities, the focus must be on identifying genuinely 'critical' capabilities (e.g. medical research) and assets (e.g. large-scale infrastructure that is essential to Australia's national interest).

At present, there is a lack of clarity on how thresholds or classification of risk would be defined or applied. Whilst there is some clarity on how the legislation would be applied to cybersecurity, there is no clarity on how it might apply to physical infrastructure, personnel and supply chain infrastructure.

Universities Australia would be pleased to work with the Department of Home Affairs to develop boundaries and thresholds for the university sector.

### ***The pandemic has tested the resilience of the university sector***

The pandemic has provided an unwelcome but effective stress test of the resilience of university infrastructure and operations. Universities pivoted, in a matter of weeks, from a mixed delivery mode of combining online and face-to-face delivery to wholly online.

The university sector has been able to deliver its educational offerings across the thousands of different courses from and to a wide range of locations effectively to students. In short, the sector, its physical and human infrastructure have been threatened and has remained resilient in the face of that threat.

### ***Challenges faced by universities***

A major shock to university capability through the pandemic has been financial through the loss of international student fee revenue, which in turn placed significant stress on universities' capacities to meet all their current commitments, and in particular research support.

Universities are also currently captured by the new *Australia's Foreign Relations (State and Territory Arrangements) Bill*, which could impact potentially thousands of research collaborations.

Physical distancing and travel restrictions have hindered some research, denying access to laboratories, major research facilities and archives. In addition to this, clinical trials and population health studies have been affected by the new demands on clinical resources and interrupted access to patients and population cohorts. Anecdotal evidence indicates that some commercial partners are withdrawing their contributions to cut costs.

Restrictions are also limiting access to partners in collaborative teams, preventing international placements, and causing the cancellation of national and international conferences. Restrictions are reducing the ability to undertake fieldwork abroad and locally, including research required to respond to urgent national needs such as the effects of the bushfire crisis.

### ***University research is a sovereign capability and underpins the nations innovative capacity***

University research capability represents a large, and until now, growing portion of Australia's R&D capacity as industry reduces its R&D activity.

Australian industry has reduced its R&D investment consistently over the last 10 years from a peak of 1.37 per cent of GDP in 2008 to 0.94 per cent in 2017 (latest). An internationally accepted measure of resilience of a country's industrial base is the level of sophistication and diversification. This is commonly proxied by what is termed the Economic Complexity Index.

Since 1995, Australia has fallen in ranking in the index from 55<sup>th</sup> (out of 133) place, to 87<sup>th</sup> place in 2018.

The scale and diversity of research capability in Australian universities provides the potential for the country to develop sovereign capability in areas of high value-added products and services.

### ***Managing and balancing the risks of foreign interference is a key priority for the sector***

Universities Australia is concerned that, with a range of legislative and regulatory programs being developed in different Commonwealth Departments, there is a considerable danger of duplication. It is essential that the 'proportionate to risk' principle is respected across the range of Government programs affecting universities. This principle must be at the centre of any decisions to layer more, potentially duplicative, regulation (with accompanying compliance costs) onto the university sector.

There is a prospect that the effect of imposing multiple sets of compliance obligations from different parts of Government will increase underlying risk rather than lessen it, with university effort diverted to addressing multiple overlapping regulatory frameworks. This would be counterproductive to the agreed shared policy objective of minimising and mitigating underlying risk.

UA would be pleased to work with the Department to identify specific issues and ways to address them.

Universities Australia and member universities have been working collaboratively with Government Departments and security agencies through the University Foreign Interference Taskforce (UFIT) Steering Group. UFIT has developed the Guidelines to Counter Foreign Interference in the Australian University Sector (the Guidelines).

The guidelines take a proportionate, risk-based approach to foreign interference and cover:

- cyber security;
- research and intellectual property;
- foreign collaboration; and
- culture and communication.

The Guidelines are designed to evolve. UFIT is successful because it is collaborative, with both Government and the university sector seeking to understand issues and address them in a sector-specific way. This partnership approach has improved security and resilience and has proved a useful alternative to regulation.

As identified in the Education, Research and Innovation workshop on 31 August, the Guidelines are an important mechanism for dealing with foreign interference.

### ***Avoid duplication of regulation and take a risk-proportionate approach***

It is important that Government work with the university sector to find the optimal balance between protecting critical infrastructure, other necessary regulation, and allowing the maximum amount of university funding to be directed towards core business – education and research.

Universities have highlighted potential duplication of regulation in export controls. The Department of Defence, through the Defence Science Partnerships Program 2.0 and the Defence Industry Security Program (both of which tie to defence research funding), already address cyber and physical security. This approach is an example of a risk-proportionate approach as defence research is a potential target for cybercrime and IP theft.

The proposed sector-specific standards approach is a 'blanket' approach and not proportionate to risk. The proposed approach would either duplicate the existing Department of Defence system, or potentially introduce another system.

The cybersecurity obligations articulated in the consultation paper are consistent with established risk management frameworks. There is no need to develop new frameworks for managing cyber security risk.

Another area of concern is the intent to oversight supply chains and reliance on offshore operational technology suppliers and expertise. As currently expressed in the consultation paper, this would be difficult to put into practice.

### ***Regulatory impact needs to be appropriately costed and implementation timelines tailored for sector maturity***

The greatest shock to research capability has been the loss of research funding due to the loss of international student fee revenue during the pandemic. Universities are under extreme financial pressure and face losing significant research capability and capacity, including a significant number of the research workforce.

Over time, government sources of funds available for university facilities and infrastructure have been withdrawn.

In this environment, additional regulatory burden on the sector will be acutely felt. It is therefore essential that regulation is well targeted, focussed and efficient.

Significant progress has been made in the university sector in building the resilience to foreign interference and other threats. UA encourages the Government to work with the sector in developing an approach and timeline that reflects the sector's maturity on these issues.

Consideration is required to ensure a sustainable approach to the regulatory burden that may be placed upon the sector, including suppliers common to the sector.

## CONCLUSION

Universities Australia strongly advocates for thorough consultation prior to the legislative amendments, and for the scope of the *Education, Research and Innovation* sector, as applied to universities, to be narrowed to focus on critical capabilities and assets.

While universities may contribute some critical infrastructure under the Act, universities in and of themselves should not be captured by the Act.

UA would be pleased to work with the Government in defining the scope and appropriate thresholds.