Innovative Research Universities

IRU submission outline - Security Legislation Amendment (Critical Infrastructure) Bill 2020

IRU position

The Government's recognition that higher education and research infrastructure is vital to the Australian economy is positive. Universities stand to benefit from a stable and secure national asset portfolio. For international collaborative research, such security will only strengthen Australia's position as a leading partner and host of research.

The emphasis on cyber security rightly targets an area of great concern where the university commitment to openness and sharing of information to advance knowledge, runs against actors which would disrupt our operations.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill) is a cumbersome means to achieve this end, for universities and likely for other sectors to be included.

Fundamentally it ignores that universities are just as keen as the Federal Government that their operations are not put at risk. Universities are active in working with the Government to reduce risks and to act when incidents occur. The major challenge is the plethora of government agencies requiring action from universities with no coherence to these requirements.

The detail of how the proposed security arrangements would work is yet to be explicated. The overall sense is that the Bill enforces action to ensure universities, as part of national infrastructure, are protected. However, it is clear that universities already respond to government information and requests and take advantage of all advice provided.

Recommendations

The IRU recommends:

1. universities be removed from the Bill and that the Government instead work collaboratively with existing bodies such as UFIT and AHECS to establish a proportionate response based on the level of individual institution risk to attacks on critical infrastructure.

If universities are not removed from the Bill:

2. the Government should, in advance of the Bill being tabled, agree with the university sector how the requirements will be implemented. The process should emphasise proactive cooperative action, ahead of enforced regulatory action, and a realistic timeframe. A sector-wide working group, building on the existing mechanisms is the appropriate means to do this; and
3. the Government should only take direct action over a university's assets in a case of extreme risk, with consent from the Vice-Chancellor.

Innovative Research Universities

What the bill proposes

The Bill proposes changes to the Security of Critical Infrastructure (SOCI) Act 2018.

The current Act:

- creates a register of information in relation to critical infrastructure assets (the register will not be made public);
- requires relevant bodies to provide information in relation to the asset, and to notify of events of concern;
- allows the Minister to require the relevant bodies to do, or not do, things there is a risk to security;
- allows the Secretary to assess the risk to national security for each asset.

The Bill will extend the coverage of the Act to higher education and research as one of eleven new sectors. It greatly extends the array of requirements under the Act. In addition to those listed for the current Act the amendment Bill:

- requires relevant organisations to have, and comply with, a critical infrastructure risk management program;
- requires notification of cyber security incidents and imposes enhanced cyber security obligations;
- sets up a regime for the Commonwealth to respond to serious cyber security incidents.

The current Act is 62 pages long, the sections in the Bill amending the current Act are 128 pages, such that the Act will be more than twice the size if the Bill is passed. The emphasis on responding to cyber security makes sense against the evidence of several serious cyber-attacks in recent years, at least one involving a university (ANU). However more information is needed to show why the current requirements of the Act are insufficient for it to achieve its purposes – for the sectors currently covered or for those proposed to be included.

Impact on universities

Is the Bill necessary?

The IRU questions whether universities need to be included in this bill to achieve the intended outcome of institutions well prepared for actions against them and able to respond in concert with government should incidents happen.

It is not clear what has happened since the passage of the *Security of Critical Infrastructure (SOCI) Act 2018* to suggest that universities are not responding effectively to advice and warnings concerning potential actions against them.

Existing mechanisms that could be used to strengthen arrangements

There are several existing relevant vehicles that could lead development and implementation of protective actions.

- The Government's University Foreign Interference Taskforce (UFIT), which includes representation of 10 government agencies and 13 universities, is the high-level body able to deal with the threat environment in a co-ordinated and meaningful way. It is possible that membership will need to be expanded to include those universities with major critical infrastructure, which would involve the Government being specific about which pieces of critical infrastructure it is most concerned about. An expanded UFIT would be a far better, less costly and more successful solution than the current bill.
- The Council of Australasian University Directors of Information Technology (CAUDIT) has partnered with Australia's Academic and Research Network (AARNet), AusCERT, Research and Education Advanced Network New Zealand (REANNZ) and the Australian Access Federation (AAF), to establish the Australasian Higher Education Cybersecurity Service (AHECS).

  AHECS is already working to support universities to continue to operate in the face of cyber disruptions. This includes awareness raising training, benchmarking, maturity assessments, coordinated threat intelligence and a sector-specific SOC provided by AARNet. These actions will help safeguard the intellectual property, digital assets, people, and hence reputation of Australia's universities.

Designed to suit the breadth of the university and research sector

It is not appropriate that all universities, whether small and based in a regional area or city based with large numbers of international students, and the different sets of research infrastructure be treated in the same way.

To work out with universities an effective strategy and its implementation would provide the risk-based and proportionate approach Universities Australia argued for in the initial round of consultation on this issue. This should be a cooperative venture without legislation but could be a system backed by a legislative framework.

New government powers for intervention

There are new powers in the Bill for the Government to "provide direct assistance to industry in the event of a serious cyber security incident." The earlier round of consultation in September 2020 raised concerns about the extent of these proposed new government assistance powers that could involve an extensive intervention in university operations.

With an effective scheme of response worked out with the sector, as proposed above, there should be little need to order actions. Rather there will be effective joint action by university and security agencies.

This means that direct government action should be used only for an extreme risk and require the approval of the relevant executive authority, most likely the Vice-Chancellor.

Linked to a whole of government approach to universities and national security

The Bill is one of several government interventions with universities as part of its response to external threats to national security. However, there is little evidence that a joined up, whole of government approach, with communication between government agencies, has been applied in this bill.

Innovative Research Universities

About the IRU

Innovative Research Universities (IRU) is a coalition of seven comprehensive universities committed to innovation and inclusive excellence in teaching, learning and research in Australia.

The members' impact is local and global with a focus on advancing communities through education, resources, opportunities, translational research and enterprise.

Through its members working collectively, the IRU seeks to be at the constructive centre of Australian university policymaking.

The membership is Charles Darwin University, Flinders University, Griffith University, James Cook University, La Trobe University, Murdoch University and Western Sydney University.

27 November 2020