Protecting Critical Infrastructure and Systems of National Significance consultation

27 NOVEMBER 2020

The Australian Technology Network of Universities (ATN), in collaboration with The University of Newcastle, welcomes the opportunity to comment on the exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

ATN is the peak body representing Australia's five most innovative and enterprising universities: Curtin University, Deakin University, RMIT University, University of South Australia, and University of Technology Sydney. Together, we are home to over 265,000 university students. The University of Newcastle is also an important community institution in the regional gateway city of Newcastle. References to ATN below should be read as representing all six universities.

The security of critical infrastructure is vitally important in the face of current and emerging sophisticated threats to Australia. It is the responsibility of the Government to set the standard in these matters, and universities have demonstrated that they are willing and able to take on proportionate responsibility and protective measures.

We welcome the opportunity to work with the Department of Home Affairs to design and implement these reforms for universities. Universities are best placed to know and understand the risks and vulnerabilities within their own organisations. We can better implement these security requirements if the Government works with us to fully understand the impact of these requirements and the support we need.

The best outcome for Australia's prosperity and security will be a risk-based and proportionate system that builds on the risk management and protections universities already have in place, adequately supported by the Government through positive mutual obligations.

ATN supports the recommendations outlined in the Universities Australia submission, in addition to our own recommendations.

Recommendations

1. The Government should define and narrow the scope of coverage through a consultation and co-design process to achieve the outcome of risk-based, targeted and proportionate protection.
2. The Government supports the reforms through positive mutual obligations in collaboration with universities, including investment in shared infrastructure and personnel.
3. The Government recognises that higher education and research infrastructure is often under shared ownership or control, and shared with external partners, and takes this into account when designing the reforms.
4. There should be a clear and shared understanding of where the boundaries are between the responsibilities of federal and state governments, regulators and entities.
5. That incident reporting obligations also be proportionate so that the effort and investment are effectively targeted at the areas of most significant risk and impact.

Risk-based, targeted and proportionate approach

ATN supports a risk-based, targeted and proportionate approach to protecting our critical infrastructure, through existing frameworks and systems wherever possible.

This approach should be defined through consultation and co-design before the Bill is introduced to the Parliament. This would provide the opportunity for the Parliament to properly consider the scope of the protections and the full impact on universities. The current approach of making the rules in delegated legislation means universities cannot effectively assess the potential impact and resources needed to comply with their obligations and the Parliament cannot make an informed decision.

A broad and untargeted approach to designating critical infrastructure and entities (and the assets within them) risks diluting the effort and attention paid to aspects that are truly critical. Universities often have multiple campuses, research centres and facilities and there needs to be consideration of the varying levels of criticality and interconnectedness.

Applying the highest level of protection to all parts of universities because of the criticality of one part would not be proportionate. An appropriate and managed ringfencing of the necessary parts would support a constructive, measured and achievable approach from universities.

Universities are in the best position to know, understand and implement the protections that are required for critical infrastructure. They can best do this with the guidance and support of the Government and its agencies.

The collaborative development of guiding principles in this space will be required, addressing example areas like the sensitivity of the research, the systems the research will be conducted on and connected to, and protection and commercialisation of intellectual property.

A unilateral determination that university IT systems or business-led applications are critical education asset, without due consideration for the scale, impact and complexity of the required work, would be harmful. There would be significant financial and opportunity costs that would affect universities' ability to deliver outcomes for students, businesses and other partners.

It is currently unclear what the process and criteria are for designating critical infrastructure, how universities would be included as partners in this process, and what opportunities there are for review and due process. For example, Minister's decisions regarding response to serious cyber security incidents (Part 3A in section 45 of the Bill) are not subject to administrative review.

Positive mutual obligations

ATN recognises that the protection of critical infrastructure is a priority for the Government and one for which there is shared responsibility with universities. Protecting critical infrastructure is important, however it is also important not to underestimate the assistance and support that may be required to achieve the comprehensive and extensive aims set out in these reforms.

Co-designing positive mutual obligations, that is mutually agreed actions and responsibilities for the Government and universities, would be a significant step towards achieving these reforms. This would need to involve Government investment in infrastructure and personnel to deliver the necessary capabilities to meet the requirements foreshadowed in the Bill.

This could take the form of resources and expertise shared across the sector to ensure the effective and consistent implementation of the reforms, similar to other examples of cooperation between the Government, its agencies and the university sector. Government contributions may take the form of incentives for investment in infrastructure and personnel.

The similarity of the assets, risks and challenges across Australia's public universities, means shared resources for protecting critical infrastructure would be an effective approach to the aims set out in these reforms. If the onboarding of shared resources was facilitated and supported, a mature and comprehensive sector-wide approach could be achievable.

As the earlier consultation paper states, "By focusing on outcomes, the new framework will ensure consistent security standards across all sectors without unnecessary regulatory impost." The outcome of protecting critical infrastructure is of prime importance, rather than replicating the same structures within or across sectors.

The higher education sector has already demonstrated that it can work positively and constructively in partnership within the sector and with the Government through bodies such as the University Foreign Interference Taskforce (UFIT). Further consultation should explore what can be learned from other programs like the Defence Industry Security Program (DISP).

Shared infrastructure

Aligned with the potential for shared resources noted above, it should be appreciated that the ownership and management of infrastructure in this sector is often at a sector-wide level or with multiple partners. For much of this shared infrastructure, while the host organisation provides base control and security, the role and purpose of these large-scale shared facilities can present challenges from the perspective of singular effective control model. In that way, this sector is perhaps unlike some of the others under consideration that have more streamlined and straightforward operating structures.

The open and shared nature of university infrastructure is a result of a sustained push from the Government over many years for universities to partner with businesses (especially small-and-medium enterprises) and to ensure that limited public resources are used efficiently. We have found that collaboration and innovation work best when our campuses are open to the public and we share our spaces and resources with start-ups and entrepreneurs. When implementing these reforms the Government needs to work with universities to preserve this culture of collaboration, integration and innovation.

For example, the National Collaborative Research Infrastructure Strategy (NCRIS) is a national network of world-class research infrastructure projects that support high-quality research that will drive greater innovation in the Australian research sector and the economy more broadly. Projects support strategically important research through which Australian researchers and their international partners can address key national and global challenges. In order to achieve the aims set out in these reforms, additional assistance and support would have to be provided for NCRIS.

Coordinated and clear approach to responsibilities

The intent towards positive security obligation is welcome and the principles-based approach is sensible. However, there needs to be a clear alignment of the various security mechanisms, regulations and requirements and a thorough assessment of the existing controls that apply in the sector.

For example, there are significant overlaps with the foreign interference and Defence Industry Security Program (DISP) certification requirements. These overlaps include the need for enhanced governance, personnel, cyber and physical security; and to declare foreign interest and ownership issues (e.g. DISP AE250-1 Foreign Ownership & Control Information (FOCI) form).

There should be clear and agreed definitions of roles and responsibilities. It should be clear where the boundaries are between federal and state government responsibilities, regulator responsibilities and entity responsibilities. Without this it is difficult to comment on actions permissible by the Government and under what conditions.

Alignment of critical infrastructure, foreign interference and DISP regulations and guidelines is critical in creating a resilient, effective and manageable university ecosystem.

Cyber security reporting obligations

The intent for reporting significant cyber security incidents is aligned with existing legislation domestically, and globally with cyber security reporting obligations. However, the time to report significant cyber security incidents (for higher education and research) represents an ambitious timeframe.

Furthermore, the current wording of the Bill could extend 'other cyber security incidents' to include all university cyber security incidents being reported within 24 hours. It is also unclear how this obligation interacts with universities' other reporting obligations, such as those that apply for foreign interference or data privacy breaches.

We would welcome clarification of the scope and definitions of cyber security reporting to ensure the intent of the legislation is targeted, and further support through additional Government funding. The rationale for this is to ensure that the effort and investment is focused on dealing with the areas of critical need and higher risk.

Additionally, while this Bill creates a positive cyber security obligation on institutions there are no concomitant protections for such disclosures. Responsible disclosures should be afforded protection.

ATN would welcome the opportunity to provide further information on any of the points raised in our brief submission, if requested. We look forward to more opportunities to engage with the Government on the important issue of protecting critical infrastructure.

Yours sincerely,

Luke Sheehy
Executive Director

Australian Technology Network of Universities (ATN)