ATN SUBMISSION

AUSTRALIAN TECHNOLOGY NETWORK OF UNIVERSITIES

Protecting Critical Infrastructure and Systems of National Significance consultation

16 September 2020

The Australian Technology Network of Universities (ATN) welcomes the opportunity to comment on this consultation paper.

ATN is the peak body representing Australia's four most innovative and enterprising universities: Curtin University, RMIT University, University of South Australia (UniSA), and University of Technology Sydney (UTS). Together, we are home to nearly 200,000 university students.

The following are general responses relevant to the education, research and innovation sector.

Risk-based and proportionate approach

Protecting critical infrastructure is important, however it is important not to underestimate the assistance and support that may be required to achieve the comprehensive and extensive aims set out in the consultation paper.

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

A broad and untargeted approach to designating critical infrastructure and entities risks diluting the effort and attention paid to aspects that are truly critical. Universities often have multiple campuses and 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.

This could include learning from other programs like the Defence Industry Security Program (DISP).

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.

Shared infrastructure

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.

8/1 Geils Court Deakin ACT 2600
E: info@atn.edu.au
T: +61 2 5105 6740
Follow us @ATNunis

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 the consultation paper, additional assistance and support would have to be provided for NCRIS.

Shared resources

This shared infrastructure, and 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 the consultation paper. If the onboarding of shared resources was facilitated and supported, a mature and comprehensive sector-wide approach could be achievable.

As the 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).

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 (FI) 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 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.

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.