ATN SUBMISSION

AUSTRALIAN TECHNOLOGY NETWORK OF UNIVERSITIES + THE UNIVERSITY OF NEWCASTLE AUSTRALIA

PJCIS review of Critical Infrastructure Bill

12 February 2021

The Australian Technology Network of Universities (ATN), in collaboration with The University of Newcastle, welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's review 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, The University of South Australia, and The University of Technology Sydney. The University of Newcastle is also an important community institution in the regional gateway city of Newcastle. Together, we are home to over 300,000 university students. 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. Universities have long understood and accepted it is the responsibility of the Government to set and enforce the standard in these matters, and we, as partners in these endeavours, have demonstrated that we are willing and able to take on proportionate responsibility and protective measures.

Over the last couple of decades, Australia's universities have adapted to and met the rising challenges faced by Australia in an interconnected and interdependent world. ATN recognises that a safe and secure Australia is important for our collective prosperity. It is important to acknowledge that, to date, the interests of both the Government and universities have best been met where the risk protection framework has been co-designed by both parties.

We welcome the opportunity to work with the Department of Home Affairs to design and implement these reforms for universities, as flagged in the Bill's draft Explanatory Memorandum. 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. Where it is possible to do so, transparency should be maintained so that all parties (Government, higher education, and others) responsible for protecting critical infrastructure can consult with each other, share best practice and build a network of protections.

Recommendations

1. The protection of critical infrastructure needs to be part of a cohesive and coordinated approach by the Government across all its agencies. The University Foreign Interference Taskforce (UFIT) should play an important role in this approach.

2. A risk-based, targeted and proportionate approach should be adopted to make efficient use of limited resources and protect the most critical infrastructure.

3. The Government and higher education sector should agree on positive mutual obligations, which are agreed commitments by the Government and universities to take on appropriate actions and responsibilities.

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

Key Points

1. ATN affirms that national security (including critical infrastructure) is the Government's solemn responsibility and universities are ready, willing and able to do their part.
2. Much of the critical infrastructure in higher education has shared ownership and management, which is a result of universities pursuing opportunities for collaboration to make the most efficient use of public resources.
3. The regulation of the critical infrastructure requirements needs to be clear and implemented with an understanding of the higher education sector and the other regulations in place.
4. Where possible, transparency should be maintained so that all parties responsible for protecting critical infrastructure can consult with each other, share best practice and build a network of protections.
5. Providing shared resources – both personnel and infrastructure – for the higher education sector is an effective way of ensuring robust and consistent protections across the sector.

Recommendation 1: The protection of critical infrastructure needs to be part of a cohesive and coordinated approach by the Government across all its agencies. The University Foreign Interference Taskforce (UFIT) should play an important role in this approach.

The responsibilities of the Government to safeguard national security are more important than ever. Over the last couple of decades, Australia's universities have adapted to and met the rising challenges faced by Australia in an interconnected and interdependent world. During this time the need for both protection and enforcement and the Australian public's trust in those systems has increased and matured.

ATN recognises that a safe and secure Australia is important for our collective prosperity and to ensure Australian society can continue to be open and engage with the world. As this maturation of national security policy has transpired, there has been an increase in Government regulation and oversight, as well as increasing awareness and management of risks by universities themselves.

The intent of introducing a positive security obligation is welcome and the proposed 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 the need to declare foreign interests and ownership.

There should be clear and agreed definitions of roles and responsibilities. The boundaries between federal and state government responsibilities, regulator responsibilities and entity responsibilities should be clear so all elements of system can function effectively. Alignment of critical infrastructure, foreign interference and DISP regulations and guidelines is critical in creating a resilient, effective and manageable university ecosystem.

The best example of a collaborative and coordinated approach to these issues is the establishment of UFIT by the Government to provide better protection for universities against foreign interference. UFIT brings together universities and a range of Government agencies – the various groups comprise around 40 members across Government and the sector, representing 13 universities and 10 Government agencies.

The Chair of the UFIT Steering Group is from the Department of Home Affairs and the Deputy Chair is Martin Bean CBE, Vice Chancellor of RMIT– this ensures that it is a genuine partnership and collaboration between the sector and the Government. It has brought together various arms of Government including the Department of Home Affairs, the Attorney-General's Department, the Department of Defence, and the Australian Security Intelligence Organisation.

The key pillar to UFIT's success is the social compact that has been established between the sector and the Government – working together as partners of equal standing. The process has been collaborative and has delivered guidelines that are applicable, scalable and implementable for all universities.

One of the key successes of UFIT is the better networks and two-way information sharing between the sector and the Government. This has enabled quick, coordinated and effective action to address emerging threats. This has already been borne out in one university being able to provide advance warning to others based on an ongoing cyber security incident.

The UFIT Guidelines make clear the importance of mature governance and risk frameworks, building a positive culture of security, proper due diligence processes, and knowledge sharing between universities and security agencies. This provides the assurance that universities and the Government need.

UFIT is the best model of collaboration and cooperation between universities and the Government. There is an excellent opportunity to take advantage of the network and relationships that have been built up through UFIT and extend this to a more holistic approach that covers all elements of national security for the sector.

ATN proposed principles and guidelines to shape cooperation between the Government and the sector are:

- Ongoing role for senior leadership in the university sector to work in partnership with the Commonwealth and the security agencies on monitoring and refining policy settings as necessary change is required.
- Data and information sharing between the Government, its agencies and its trusted university partners to allow faster and more effective identification of risks and protections against threats.
- More collaborative and partnership-based initiatives like UFIT are vital for the Government and its agencies to understand the particular risks and challenges within the university context.
- If the Security Legislation Amendment (Critical Infrastructure) Bill 2020 passes the Parliament, the co-design process to design the sector-specific Positive Security Obligation will be important, as will additional investment in personnel and infrastructure.
- Any protections and controls should not only be risk-based and proportionate, but also function in timely and efficient way in order to maintain Australia's global competitive advantage.
- There should be consistency and coordination across the various protections, controls and legislative frameworks. Co-design and consultation need to take into account not only specific initiatives (e.g. critical infrastructure protections), but also how they interact and overlap.
- There should be ongoing consultation between the sector and the Government (through bodies like UFIT) to help strike a balance between beneficial research collaboration and security concerns so that regulation is not overly restrictive and greater than necessary to achieve the government's policy objectives.

Recommendation 2: A risk-based, targeted and proportionate approach should be adopted to make efficient use of limited resources and protect the most critical infrastructure.

ATN supports a risk-based, targeted and proportionate approach to protecting our critical infrastructure, through existing frameworks and systems wherever possible. The sector is highly aware of the national security risks and has taken positive steps to mitigate and address these risks, while continuing to provide world class teaching and research that benefits Australia.

Universities have worked closely with the Government on these issues, including through UFIT, the Foreign Influence Transparency Scheme (FITS), the Defence Industry Security Protocol (DISP), and the *Defence Trade Controls Act 2012*.

Universities have a deep understanding and appreciation that the need for security applies across a broad spectrum of activities, from data and personal information through to national critical research infrastructure.

Universities face similar risks (and similar scales and impacts of risk) regarding data theft and espionage to any Australian public institution or company, and that is why we have appropriate defences in place. These defences are proportionate and risk-based – ensuring that the protections are targeted to the areas of highest need and most criticality.

The majority of the research output of universities is designed and intended to be publicly available, as this contributes to our missions of furthering knowledge and improving society. While universities do undertake research of a sensitive nature, regarding defence and national security, this research is subject to appropriate protections applied and overseen by universities, the Government and its agencies, and any other parties involved.

Research is fundamental to improving Australian society and the economy. It is therefore essential that an appropriate balance is struck so that security concerns are responded to and beneficial research collaborations continue.

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. Finite security resources should be directed to the areas of greatest risk and potential impact, such as defence research partnerships. 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.

Building on the collaboration and cooperation between universities and the Government through UFIT would be ideal to tackle these issues in a comprehensive, consistent and measured way. This would make it possible to develop a risk-based, targeted and proportionate approach that is backed by mutual understanding and responsibility.

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.

Without such a collaborative approach, the protections imposed may not be feasible or implementable. For example, a unilateral determination that university IT systems or business-led applications are critical education assets, 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.

Recommendation 3: The Government and higher education sector should agree on positive mutual obligations, which are agreed commitments by the Government and universities to take on appropriate actions and responsibilities.

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. 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.

Protections and security infrastructure are often shared across universities in order to deliver comprehensive, consistent and scalable solutions, and best value for investment for the Government.

Example: Establishment of the AARNet Security Operations Centre (SOC)

The AARNet SOC is a purpose-built facility that provides Australian universities with all the capabilities they need to manage cyber security incidents. Real-time monitoring and data analysis combined with incident co-ordination and remediation support helps protect campus networks, assets and people from cyber threats. This provides improved information sharing and coordinated responses across the sector – this can prevent and address threats such as email phishing attacks.

Example: Australian Higher Education Cybersecurity Service

AARNet, Council of Australasian University Directors of Information Technology (CAUDIT) and AusCERT are partnering to coordinate an Australian Higher Education Cybersecurity Service (AHECS), aligning activities with the aim of safeguarding the reputation of the higher education sector through coordinated, complementary cybersecurity-related portfolios of activity. This includes many initiatives, but of particular note are: shared third party product/vendor due diligence and risk assessment by establishing a HECVAT (Higher Education Community Vendor Assessment Toolkit); and sharing of threat intelligence across the sector in an automatic and consumable manner.

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.

There is significant cyber security expertise and capability within Australia's higher education sector – we have some of the world's leading researchers in this space and they are already working with the Government and businesses both large and small. However, extra resources and support will be needed to turn these world leading insights into practical protections.

Example: Deakin's Centre for Cyber Security Research and Innovation (CSRI) was established in 2017 and develops innovative technologies and methodologies for securing cyberspace in Australia and beyond.

CSRI solves the cyber security threats of tomorrow by working with industry and government leaders on innovative research that has real-world impact. Researchers in CSRI represent a diverse section of academic fields, spanning all of Deakin's faculties. The CSRI team also includes Adjunct Industry Professors who are experts and leaders working within the private sector and government. This holistic approach to cyber security research means CSRI is uniquely positioned to collaborate and innovate in meaningful ways to improve security of governments and the Australian community.

Deakin researchers are working with the Department of Home Affairs to assist in the development of best practice guides that will be used across Australia to protect the expanded critical infrastructure sectors from various threat vectors (e.g. physical, cyber, personnel and supply chain).

The centre also specialises in research on cybernetics, artificial intelligence, information warfare, organisational and infrastructure security, privacy and identity management, and strategic policy. A new research pillar focused on defence has been established and is working with the Defence Department's Defence Science and Technology (DST) Group and the United Kingdom Ministry of Defence.

Example: RMIT's Centre for Cyber Security Research and Innovation (CCSRI) was established in 2020 with a focus to develop a multi-disciplinary research centre relating to the organisational, human and technology aspects of cyber security. The CCSRI is leading a project with UFIT on behalf of the higher education sector. It will manage the project as part of the Government's cyber security grant of $1.6 million to enhance the cyber security of Australia's universities.

Deakin's CSRI and RMIT's CCSRI recently partnered with Cynch Security to produce the 2021 State of Cyber Fitness in Australian small businesses white paper. This research looked at the cyber security risks facing small businesses, how prepared they are, and how their 'cyber fitness' can be improved. A similar approach will be needed across many of the sector that will be now designated as critical infrastructure.

One of the points in the paper is that small businesses are part of supply and value chains that involve much larger businesses with higher levels of cyber security maturity and flexibility. This illustrates the reality that protecting critical infrastructure extends far beyond the designated institutions and sectors – it extends to their partners, suppliers and end-users.

As such, critical infrastructure protections must be implemented and built up in a carefully planned and stepped approach. Our approach must be a combined one with the Government and must be sustainable, well resourced, and allowed to adapt and mature as it progresses.

Further enquiries should be made to:

Executive Director
Australian Technology Network of Universities
+61 2 5105 6740