Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector

18 DECEMBER 2020

The Australian Technology Network of Universities (ATN), in collaboration with The University of Newcastle, welcomes the opportunity to make a submission to the inquiry by the Parliamentary Joint Committee on Intelligence and Security into national security risks affecting the Australian higher education and research sector.

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

The Government's responsibilities in safeguarding our national security have grown out of necessity over the last several decades. During this time the need for both protection and enforcement and the Australian public's visibility of such has evolved. ATN believes in this central tenet of national security policy, that national security is now, and always has been, within the purview of the Government to both protect and enforce. As these considerations have developed, Australia's university sector has been in lock step with the Government in fulfilling Australia's needs.

Australia's university sector has adapted to and met the rising challenges faced by the impact of these solemn and necessary issues. 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 the university sector have been met, where the risk protection framework has been co-designed by both parties. Australia's university sector and ATN members are willing partners in these pursuits.

RECOMMENDATIONS

- Best practice is achieved where risk-based, targeted and proportionate protection is implemented and to date the best way to achieve this has been through consultation and co-design between the Government and the sector.
- A holistic approach is needed across all national security governance and regulation to ensure that the protections are comprehensive, coordinated, and proportionate.
- A risk-based, targeted and proportionate framework demonstrates a clear and shared understanding of where the boundaries are between the responsibilities of various federal and state governments, regulators and other entities.
- Where there are positive mutual obligations between Government and universities that enable the protection of national security, these should be supported, including through investment in shared infrastructure and personnel.
- To provide a timely and effective responses to emerging threats, two-way data and information sharing between the Government and trusted partners should be considered.
- The Government should use the University Foreign Interference Taskforce (UFIT) as the focal point for tackling foreign interference and related issues to build on the genuine partnership between Government and universities.

KEY POINTS AND OBSERVATIONS

- The world has experienced an elongated period of disruption relating to national security and the ways in which Government, businesses and universities respond have evolved out of necessity.
- National security is vitally important in the face of the current and emerging sophisticated threats to Australia. It is the responsibility of the Government to set the standard in these matters.
- Australia's university sector has been a willing partner in these solemn and necessary issues.
- Universities recognise that a safe and secure Australia is important for our collective prosperity.
- Universities have demonstrated that they are willing and able to take on proportionate responsibility and protective measures. This is evident in the positive measures universities have implemented independently, in partnership with each other, and with the Government.
- Universities are public institutions, existing for public good, which means we have a responsibility to ensure national prosperity, and the development of knowledge, as well as a critical role as custodians of our free and open society.
- Universities are open places which foster free intellectual inquiry and expression. This openness is a core part of how universities succeed and contribute to Australia's liberal democracy.
- The existing and incoming regulatory and legislative framework governing the operations of universities is significant, rigorous and effective – particularly in relation to foreign arrangements, critical infrastructure, foreign interference transparency, defence trade controls, defence industry security protocols and UFIT. It is made more effective when it has been developed in close partnership between Government, security agencies and the sector.
- Australian universities are globally connected, but local grounded – our international partnerships and networks are vital for us to continue to deliver the world-class research and teaching that benefits all Australians.
- Mutual understanding goes hand in hand with mutual obligation, that is why universities take national security matters with the utmost seriousness and have, particularly over the past two decades, developed better culture and practice to reflect our obligations and responsibilities in protecting the nation.
- Given the global nature of the challenges presented by the evolving national security policy landscape, Australia's Five Eyes partners have all moved in recent times to scaffold and supplement existing proportionate, targeted and risk-based frameworks. In many ways, Australia's policy framework is in line with our friends and allies. Where changes flagged have exceeded that of our closest allies, the university sector has been frank with the Government and sought changes which better align with the principles of risk-based and proportionate regulation.

Responses to terms of reference

This section deals with issues raised in both #1 and #2 terms of reference:

#1 The prevalence, characteristics and significance of foreign interference, undisclosed foreign influence, data theft and espionage, and associated risks to Australia's national security; and

#2 The Sector's awareness of foreign interference, undisclosed foreign influence, data theft and espionage, and its capacity to identify and respond to these threats

- To achieve the best outcomes in safeguarding our national interests through the development and implementation of national security policy, universities have been willing partners with Government. This has been most effective where the sector has participated, in partnership, in the co-design of risk-based and proportionate measures that align with measures implemented by our allies and partners globally.
- ATN looks forward to continuing to work closely and in consultation with government and business to implement and monitor policy settings to ensure they are effective, have mutual understanding and obligations, drive a culture of awareness across our sector and strengthen, rather than diminish, Australia's open and world-affirming society.
- ATN would emphasise the outstanding work undertaken by Government, security agencies, and the university sector in the establishment of UFIT and the associated development of guidelines.

"...through my universities, Martin Bean has represented the sector diligently in a way that works with the needs and interests of the security agencies in the government and, of course, the processes that we have at universities. I think that's been a good model."

Mr Luke Sheehy, Executive Director, ATN

In evidence to Senate Standing Committee on Foreign Affairs, Defence and Trade Inquiry into Australia's Foreign Relations (State and Territory Arrangements) Bill 2020

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, the Defence Industry Security Protocol, and the *Defence Trade Controls Act 2012*.

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. 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 and academics are proud of their academic freedoms, the exercise of which are underpinned by evidence, research and scholarship. The tradition and practice of peer review operates hand in hand with academic freedom to produce teaching and research that is robust and defensible. The open nature of our campuses and scholarly output invites fair and reasoned challenges, which strengthens our communities against untoward influences.

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 national security, this research is subject to appropriate protections applied and overseen by universities, the Government and its agencies, and any third 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.

> *"...we are working with the Federal Government and the Home Affairs security agencies around the University Foreign Interference Taskforce. We acknowledged the changing dynamics of the geopolitical state and we are also working very closely with the Government to make sure that we have the right systems and processes in place to safeguard the independence and the autonomy of our institutions while not shutting them down."*
>
> Professor Attila Brungs, Vice Chancellor of UTS, Chair of the ATN
>
> Evidence given to NSW Portfolio Committee inquiry into the Future Development of the NSW Tertiary Education Sector

CASE STUDIES OF ACTIONS TAKEN

Example 1: Specialised Expertise

UniSA

A Defence and National Security Officer has been appointed at UniSA. This person will be responsible for all security matters relating to defence research and education across UniSA. This includes the development and implementation of appropriate security governance and risk management across university functions, to meet industry security requirements and applicable to UniSA more broadly.

The role will extend beyond defence security and will work across UniSA to support staff in advancing their ideas and how they can work collaboratively with Australian and international partners within the context of often complex relationships while also protecting intellectual property. The role will undertake UniSA's commitment to obtaining Defence Industry Security Program (DISP) accreditation.

UTS and The University of Newcastle

From early 2021, a newly created Chief Information Security Officer role will be shared jointly between UTS and The University of Newcastle. This builds on the foundation set in 2019, when UTS appointed a full-time specialist resource dedicated to managing research related risks, including foreign interference, defence trade controls, and intellectual property leakage.

It also builds on recent initiatives taken by The University of Newcastle, as the first university in Australia to move its data entirely into the cloud. Coupled with a new system of double authentication, this has significantly improved not just resilience but also security of data. The University is working across the sector to assist other universities adopt these measures.

Example 2: 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 3: 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)
- Sharing of threat intelligence across the sector in an automatic and consumable manner.

Example 4: RMIT University Centre for Cyber Security Research and Innovation (CCSRI)

The 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.

Example 5: Deakin University Centre for Cyber Security Research and Innovation (CSRI)

Established in 2017, 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 uniquely positions CSRI to collaborate and innovate in meaningful ways to improve security of governments and the Australian community.

Deakin researchers are working with 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.

To enable advanced industry engagement and collaboration, Deakin also runs the Executive Advisory Board for Cyber (EABC) which comprises 46 leading Australian organisations and government departments which meets quarterly to discuss various topics.

Example 6: Increasing cybersecurity awareness and upskilling staff at UTS

The recently refreshed Cybersecurity Standards at UTS provide guidance on how to balance the need to protect information technology assets, work efficiently and meet regulatory and legislative requirements. They cover measures all staff need to take, including the use of passwords and the classification of information. The Security Awareness Uplift project also aims to raise the cybersecurity awareness culture across the University through a structured and robust Cybersecurity Communications Program.

Example 7: Risk management and governance at UTS

UTS is in the process of finalising a broad strategic risk assessment of all research activities to identify and assure its risk profile aligns with its risk appetite. Where there is disjunction, UTS is putting in place specific actions that mitigate the risk to an appropriate level. The shifting geopolitical climate and related considerations (including foreign interference and improper influence) have been identified as key drivers in our operations and risk appetite, thereby ensuring continual monitoring and actioning through appropriate governance and management channels.

UTS has launched an international engagement and collaboration portal that outlines a principles-based approach to engaging with international entities and colleagues. This portal embeds a structured approach to managing these engagements in UTS practice and ensures all collaborations are actively considered for alignment to UTS's long-term strategic direction and considered in light of applicable regulatory considerations.

#3 The adequacy and effectiveness of Australian Government policies and programs in identifying and responding to foreign interference, undisclosed foreign influence, data theft and espionage in the Sector

- There has been a necessary evolution in both Government responses and university responses to the challenges presented by national security considerations.
- Universities have been a willing partner in ensuring these challenges are met and have driven cultural and policy change across our institutions.
- We call for the development of principles to shape future cooperation between Government and universities.
- Mutual understanding goes hand in hand with mutual obligation. That is why universities take national security matters with the utmost seriousness and have, particularly over the last two decades, developed better culture and practice to reflect our obligations and responsibilities in protecting the nation.

The responsibilities of the Government to safeguard national security are more important than ever. During this time the need for both protection and enforcement and the Australian public's visibility of such has evolved. ATN believes in this central tenet of national security policy, that national security is now and always has been within the purview of Government to both protect and enforce.

Australia's university sector has adapted to and met the rising challenges faced by the impact of these solemn issues. ATN recognises that a safe and secure Australia is important for our collective prosperity and to ensure Australian society continues to be open and world affirming. As this evolution within 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.

Our Government is taking action to provide clarity at the intersection of national security, research, collaboration and a university's autonomy. ***Universities also understand the risk to their operations and to the national interest from cyber attacks and foreign interference and we are working constructively to address it.*** *[UFIT] will complement work currently underway involving Defence, other relevant agencies, universities and industry to develop practical, risk-based legislative proposals to address identified gaps in the Defence Trade Controls Act.*

Minister for Education, Dan Tehan, Development of University Foreign Interference Taskforce media release **28 August 2019**

The Government has established UFIT to provide better protection for universities against foreign interference. UFIT brings together universities and 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.

RMIT Vice Chancellor and President Martin Bean CBE, one of the co-chairs, said he was delighted to see the **shared commitment of universities and the Government to safeguard the security of Australia's university sector without undermining the invaluable asset of its openness.**

"*The guidelines are a fantastic new resource for universities to add to their existing tools and to assist decision makers in continuing to assess the evolving risks from foreign interference*," he said.

Protecting Australian universities from foreign interference media release **14 November 2019**

This has led to one of the key successes of UFIT which is greater networks and two-way information sharing between the sector and the Government. This has enabled quick, coordinated and effective action to 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.

UFIT is guided by the following overarching principles:

- security must safeguard academic freedom, values and research collaboration
- research, collaboration and education activities must be mindful of national interest
- security is a collective responsibility with individual accountability
- security should be proportionate to organisational risk
- the safety of our university community is paramount.

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 gold standard for 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.

The *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* means that the Government will be aware of any arrangement of concern between a university and foreign government partner. This will provide the Government unprecedented insight into the operations of universities, and presents an opportunity for greater sharing of information by the Government to assist universities.

We can build on the policies and programs already in place at individual universities, across the sector, and in partnership with Government.

Principles and guidelines to shape the future state of cooperation between the Government and the sector are:

- Ongoing role for senior leadership in the university sector to work 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 and trusted partners could allow faster and more effective identification of risks and protections against threats.
- More collaborative and partnership-based initiatives like UFIT will be 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 well as 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 and controls. 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 objective.

#4 Responses to this issue in other countries and their relevance to the Australian situation

Given the global nature of the challenges presented by the evolving national security policy landscape, Australia's Five Eyes partners have all moved in recent times to scaffold and supplement existing proportionate, targeted risk-based frameworks.

Since World War 2, it has been bipartisan Australian Government policy to encourage Australian businesses - including universities - to foster and build relationships with countries within our region. It has been a successful part of Australia's foreign policy during this time – leveraging our international collaborations and research partnerships to ensure that Australia has access to the cutting edge of investment in technology and breakthroughs in science. This undoubtedly continues to serve Australia well.

ATN recommends that the Government works with the sector on a proportionate and risk-based approach to managing all interactions that have a national security lens with foreign governments and related entities. A collaborative approach would be more effective at continuing to embed the responsibility for security within the operations and culture of all Australian universities interacting with international partners. This approach would be in step with Australia's Five Eyes partners.

"*Australia is maturing into an advanced knowledge-based economy. This means we need to manage our intellectual property on an international basis. The Defence Export Controls regime is an excellent framework, which forms a good starting point.*"

Professor Alex Zelinsky AO, Vice Chancellor, The University of Newcastle

In AFR article, *Universities say they are cautious with China on research*, 21 August 2019

In an ever-changing world where the risk mitigation requirements placed on businesses, government and universities have become more comprehensive and detailed, collaboration between Government and universities is integral to Australia's prosperity. ATN looks forward to working in partnership with the Government to further strengthen and support our collective endeavours.

Key contacts for this submission are:

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

Professor Alex Zelinsky AO
Vice Chancellor
The University of Newcastle
+61 2 4921 5101