Queensland University of Technology

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

Queensland University of Technology (QUT) welcomes the opportunity to contribute to the Committee's inquiry into national security risks affecting the Australian higher education and research sector. QUT endorses the Universities Australia (UA) submission to the present consultation – this document should be read as a supplement to that unified sector view.

Introduction

Like all Australian universities, QUT supports a strong and robust position in defending Australia's national interests from foreign interference. QUT has worked closely with UA as the sector lead in developing solid governance frameworks related to foreign interference and transparency. QUT commends the work of the University Foreign Interference Taskforce (UFIT) which brought together representatives from the university sector and key Commonwealth agencies.

Since the release of the *UFIT Guidelines to Counter Foreign Interference in the Australian University Sector* (the UFIT Guidelines) in November 2019, QUT has worked methodically and diligently to review and increase our internal controls to identify and counter foreign interference and influence. These internal mechanisms include: strengthening due diligence in review of research and commercialisation contracts and higher degree research; embedding checks in our human resources recruitment and appointment processes; reaffirming our commitment to a comprehensive and constantly evolving cybersecurity plan; updating policies to safeguard reporting practices; and expanding disclosure of interest procedures.

We see the UFIT Guidelines as a core tool to assist and support the sector in responding to this challenge in line with Federal Government expectations and the national interest. We note however that the UFIT Guidelines, while comprehensive and balanced, will require ongoing updating and regular communication with the Commonwealth agencies monitoring foreign interference in order to maintain currency. To facilitate this, QUT recommends more open dialogue and discussion from federal agencies on these issues with the sector – and, critically, the development, improvement and entrenchment of effective mechanisms for cross-portfolio awareness and communication between Commonwealth agencies with an interest in this space.

For the convenience of the Committee, the remainder of our remarks will be addressed to the inquiry's Terms of Reference.

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

QUT notes the vital contribution that the higher education and research sectors make to Australia's national interest and the importance of international collaborations to the success

of those endeavours. This contribution and its significance are outlined in detail in the UA submission to the inquiry, and we stand ready to provide the Committee with further specific examples of this activity and its national benefit should that be of assistance to its deliberations.

We believe that the prevalence of foreign interference and influence in the higher education and research sector is relatively low at present, although the potential risk to Australia's national security is high.

Improving awareness, transparency and openness on these matters will be the most important factor in ensuring that the sector is aware of the risks, has adequate internal controls in place and long-term capacity is built and in place to deter and deal with threats.

In relation to data theft and espionage, QUT is continually monitoring and improving its data protection capability. Some of the key activities are:

- QUT is currently executing a Cyber Security Program to provide significant maturity improvements in the areas of Community Engagement, Governance, Identity and Access Management and Technical Threat Management. As part of this program QUT is implementing an ISO/IEC 27000-compliant Information Security Management System (ISMS) and where practical adopting the controls recommended by the Australian Cyber Security Centre (ACSC).
- A comprehensive Security Testing and Vulnerability Testing program provides an accurate view of our vulnerabilities, enabling the prioritisation of remediation activities. New systems are tested prior to release as per the project lifecycle.
- QUT is highly engaged with industry peers through the Council of Australasian University Directors of Information Technology (CAUDIT) Cyber Security Community of Practice, and actively shares threat intelligence with multiple external organisations including AusCERT and the Australian Government's Joint Cyber Security Centres (JCSC).
- QUT has a multi-channel Security Awareness program to educate users about current and emerging cyber-threats.
- QUT has a consistent incident management process for managing IT incidents irrespective of their origin. Information security incidents are reported through this practice. In the case of incidents such as data breaches there are well-developed Security Incident Response processes that clearly define the roles and responsibilities during all phases of the incident – Detection, Analysis, Containment, Eradication, Recovery and Post Incident Clean-up.
- QUT has detected 600 information security incidents over the last 12 months. The main actors targeting QUT are cybercriminals seeking to compromise credentials for financial gain. While it is possible that any credentials harvested in this way could be on-sold to nation-state actors, there is no evidence to suggest this has occurred.
- The only significant nation-state activity detected by QUT in 2020 was in March when QUT was targeted by an Iranian actor known as 'Charming Kitten', that has been linked to ongoing credential collection operations, by redirecting users to false login-related websites via phishing emails. This campaign targeted a number of Universities across Australia. All of the phishing emails were detected and blocked by QUT's Secure Email Gateway.
- QUT continues to participate in sector-wide initiatives to share information and intelligence. The Australian Higher Education Cyber Security Service (AHECS) has been established in 2020. AHECS is a joint initiative between CAUDIT, AusCERT, AARNet, REANNZ, and AAF. AHECS's purpose is to establish a trusted community that leverages new and existing capabilities to mature cybersecurity across the

sector in order to safeguard the intellectual property and reputation of Australasia's universities.

- There are also well-established Communities of Practice that enable further information exchange between universities on a local level. For instance, all Queensland universities are members of REN-ISAC, which is a global higher education threat and intelligence sharing community.
- QUT is an active stakeholder of the Federal Government Joint Cyber Security Centres that provide broader advice and intelligence at a more regional level.

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

QUT suggests that following the development of the UFIT guidelines there is a much greater mutual understanding of the risks and potential issues in this space.

Having said that, it is difficult to offer a comprehensive response to this consideration absent a clear articulation by the Committee of the precise types of foreign engagements of interest to the inquiry. Many university agreements fall within the current broad scope, but may be of tangential interest to the Committee: for example, student and staff exchanges, scholarship programs and joint venture arrangements are certainly captured, but these agreements function to facilitate important operational international partnerships and most will not trigger any foreign interference or influence considerations.

Similarly, the sector will be able to come to the point of the inquiry much more effectively if candour about specific jurisdictions of concern is forthcoming. The attempt to frame this discussion in country-agnostic terms has the potential to consumes enormous energy to nil effect, by capturing some activities that are technically encompassed but pragmatically of little to no concern. For example, for the past few decades one of the major outlets of the trade press for the university sector has been the Higher Education Supplement (HES) of the national daily broadsheet. The HES is published in *The Australian* each Wednesday by News Corp, a company run by a United States citizen who has a well-earned reputation for maintaining an active interest in the flavour and influence of his company's publications.

C. 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;

The Australian Government Cyber Security Strategy was released on 6 August 2020. This strategy puts in place a much stronger defensive capability to provide protection for Australians from sophisticated threats. Some of the strategic initiatives are:

- Strengthened defensive capability at a national level;
- Improved baseline security, skilled workforce growth and growing cooperative information sharing and incident response capabilities; and
- Improved education and cyber incident reporting for individuals.

These initiatives are a good start to delivering a more secure online experience for all Australians. As the implementation of the strategy proceeds the risk of nation-state-based data theft should decrease as Australia becomes a more difficult target for successful attacks.

More broadly relating to foreign interference and influence, QUT recommends a deepening of the engagement between the higher education sector and key government agencies through more regular dialogue, the establishment of dedicated liaison positions, the

identification of single points of senior contacts in each higher education institution that have responsibility for the coordination of policy, detailed sharing of best practice, and a more open incident reporting procedure.

QUT recommends that the key definitions and functions of the agencies tasked with protecting Australia from foreign interference be made more public, and that they more actively engage in threat mitigation work with the sector.

Most gravely, there are legitimate emerging concerns across the sector about a lack of coordination and mutual awareness across Government with respect to the application of national security and foreign influence measures to universities. This not only presents universities with serious compliance challenges; it also constitutes a significant source of real risk that has the potential to undermine our collective efforts in resisting foreign interference. This Government-generate risk is currently in play, and requires urgent action to eliminate or mitigate it. The heightened risk is rendered all the more dangerous because many parts of Government seem to be unaware of it: fortunately, it is as readily eradicable as it is unnecessary.

QUT absolutely recognises the seriousness and importance of protecting Australia and its public institutions – including universities – from untoward and pernicious foreign influence, interference and injury. We also appreciate the gravity of national security matters, and the delicacy with which they must be addressed, including the need for secrecy. Our concern on this point does not go to the policy objective of securing Australia: it goes to implementation.

It is apparent from recent experience that various parts of Government are initiating measures to protect universities from foreign interference without regard for each other's proposals, let alone for the existing rigorous collaborative arrangements that are already in place. We consider it most unlikely that federal agencies would wilfully ignore related initiatives or effective existing measures, so we can only conclude that there is a lack of knowledge and understanding of what other parts of Government are doing to address common concerns in this arena.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2020* proposed by Home Affairs is a leading example, coming very soon after another relevant piece of legislation, the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* and its associated consequential amendments Act, brought by Foreign Affairs. A contextual reading of both policy proposals produces the inference that they were drafted in apparent ignorance of the effective operation of the University Foreign Interference Taskforce (UFIT), established by the Minister for Education and chaired by a Deputy Secretary of the Department of Home Affairs.

If the Commonwealth does not address this lack of coordination and line of sight between agencies and better integrate initiatives designed to counter foreign interference, there are three likely adverse effects that will result:

1. *A counterproductive elevation of underlying risk*

   Most seriously, this uncoordinated approach will produce an increase in real terms to our sector's *de facto* exposure to foreign influence, interference and malevolent attack, as universities' resources are engaged increasingly in addressing multiple overlapping but differently designed compliance protocols, with excess attention and energy devoted to rechecking every corner and ticking boxes instead of watching the gate. These overlapping compliance obligations will be the responsibility of the same officers – the effect in operational terms will be a reduction of monitoring effectiveness as multiple compliance elements are ticked off under several paradigms to cover broadly the same monitoring and scrutiny activity.

   Vigilance will suffer unless we can instead agree on a set of common activities, protocols, concerns and measures that cover all needs with good visibility for all

relevant interested parties. We have a far greater likelihood of achieving the overarching policy objective of protection from harm under a single overarching regime that meets everyone's needs than through a collection of poorly conceived, uncoordinated and blunt instruments, which is the current scenario. The Commonwealth designed UFIT to be just this kind of effective, flexible and collaborative mechanism – characterised by the sharing of good practice and the maintenance of a synoptic view of the security environment and of areas of concern – yet the Government has recently introduced entirely new regimes (such as those from Foreign Affairs and Home Affairs) as though UFIT does not exist.

The reduction in functional vigilance due to an increase in bureaucratic compliance that adds significant labour but marginal additional scope of attention is especially true in the reduced staffing environment now characteristic of universities in light of the financial effects of COVID-19. While adding compliance complexity for little to no gain is never a good idea, universities are simply not in a position at present to devote additional resources to meet the additional non-productive burden.

2. *Tension with other Government policy priorities*

   The lack of coordination has policy implications as well as the potential to hamper operational effectiveness. Some of the measures being proposed are antithetical to and actively antagonise other initiatives and priorities of Government, such as the protection of academic freedom, the encouragement of university-industry collaboration, and the imperative to conduct world-class research.

3. *Unnecessary regulatory impact*

   Each of the new regimes offered by Foreign Affairs and Home Affairs appears to have been designed in isolation, as though it were the only one addressing concerns in this domain, with the result that the mechanism in each case is both blunt and far too broad, with an unnecessarily outsized regulatory impact. A net this large will not only harvest an enormous by-catch, it is also unlikely to catch the subtle and alert target – surely a major priority of national security concern. Departments should be made aware of existing effective measures such as UFIT, the *Defence Trade Controls Act 2012* and the like, enabling them to ensure their specific concerns are met by addressing any gaps in that work to ensure the unified regime is proportional, efficient and effective, instead of arbitrary, laborious and ineffectual.

QUT proposes that the remedy for this problem is an effective inter-agency collaboration mechanism, combined with broader membership of UFIT, to identify, harmonise and develop protection regimes to ensure that all concerns are addressed. It may be that this beneficial mechanism can be enacted beneath the current legislative umbrella, but if necessary Bills and Acts may need to be redrafted or amended (respectively) in order to integrate the relevant protection requirements into the work of UFIT, in consultation with that Taskforce and the sector broadly. Thereafter if gaps are identified in university protocols and practices by Commonwealth agencies, they should be addressed in collaboration with all relevant portfolios through UFIT, rather than establishing entirely new regimes to run in parallel.

QUT argues strongly that the sector is deeply committed to protecting Australia's national interest and working on mutually beneficial programs, but the current proliferation and obscurity of arrangements are generating more heat than light. This is not only a waste of effort, it is also a genuine source of real risk by means of diverting attention and effort to the mechanics of operating in an unnecessarily complex environment. Alignment of objectives and mechanisms, along with transparency and directness of engagement, will improve efficiency and best mitigate real risk in this critical arena.