



The University of Melbourne

Submission to the

Parliamentary Joint Committee on Intelligence and Security

Inquiry into national security risks affecting the Australian higher education and research sector

December 2020

Executive Summary

The University of Melbourne welcomes the opportunity to provide input and comment to the Parliamentary Joint Committee on Intelligence and Security *Inquiry into national security risks affecting the Australian higher education and research sector*.

The University shares the Australian Government's commitment to securing Australia's national interest from foreign interference, undisclosed foreign influence, data and intellectual property theft, and espionage (for succinctness, indicated hereafter as 'foreign interference'). The University is alert to the existence of threats against Australia's knowledge and technological resources and is proactively managing these risks in our context. We recognise the need for heightened awareness in the research sector and assurances that the necessary processes and practices are in place to keep our people, systems and research safe.

Universities play an important role in Australia's global engagement through international education and research collaborations, built up over decades through mutually beneficial arrangements. These connections and partnerships deliver to the Australian people crucial access to knowledge and talent that contributes to Australia's long-term prosperity and security. Global partnerships deliver research that is beyond Australia's capacity to advance alone; brings international expertise to bear on issues of national importance; and supports research that may otherwise go unfunded. As the global environment becomes increasingly uncertain and some of Australia's key relationships in Asia more complex, universities, like other sectors, are working to navigate those challenges in a way that preserves the benefits of our international connections while safeguarding the national interest.

An extensive suite of national interest legislation regulates university activity, including laws that cover autonomous sanctions, defence trade controls, export controls, foreign influence registrations, national security legislation and critical infrastructure. These regulatory regimes underpin university activities and are the basis of our extensive compliance assurance mechanisms. Our activities are also guided by national professional codes for research integrity, such as the *Australian Code for the Responsible Conduct of Research*, as well as requirements from funding agencies such as the Australian Research Council (ARC).

On an operational level, the University and its members regularly work with different parts of the Australian Government and its agencies to identify and mitigate foreign interference risk. As a sector, Australian universities collaborated with Federal Government Departments over the last 18 months to develop the *Guidelines to Counter Foreign Interference in the University Sector (UFIT Guidelines)*. The implementation of the *UFIT Guidelines* within our institutional governance framework is contributing to greater awareness across the academy and more systematic risk mitigation. The UFIT model could be adapted to facilitate other legislative and regulatory changes and serve as the mechanism through which new reforms are implemented in collaboration with the sector.

The University has arrangements in place to support ongoing compliance under the *Foreign Influence Transparency Scheme Act 2018 (FITS Act)* and other legislation. We are refining and fortifying risk mitigation arrangements and oversight mechanisms to reflect foreign interference risks as they are known today, and as they evolve. We appreciate that the risks

may arise externally or internally; in new or existing arrangements; to different extents; and in diverse forms. In view of the complex and dynamic nature of foreign interference threats and uncertain geopolitical times ahead, the University is adopting a whole-of-institution approach to scrutinising and strengthening our systems.

This submission outlines systemic and specific efforts underway at the University to enhance risk management, including Case Studies on The Peter Doherty Institute for Infection and Immunity and The Confucius Institute at the University of Melbourne (on pages 10 and 16 respectively). It summarises how the University is enhancing physical (technology and infrastructure) preparedness and governance mechanisms; building a stronger information base to guide day-to-day decisions and enhance risk management; and reinforcing risk literacy and mitigation practises across the institution. These efforts are overseen by a Foreign Interference Working Group comprising senior leadership from across the institution.

High-quality, collaborative research is pivotal to Australia's productivity and innovation, and often involves working with, or recruiting, outstanding overseas partners. Rather than limiting or reducing international engagement, Australia's global connectivity through its university sector is well-positioned to be responsible, informed and managed, through a cooperative cross-sectoral partnership approach between universities and government that responds to changing needs around foreign interference prevention and risk management.

Future regulation should be co-designed through the partnership prism, proportionate to the risks and balanced against the significant value that international engagement delivers to Australian society and beyond. Disproportionate interventions could undermine the economic and social benefits and positive impact of our international activities while not necessarily enhancing national security.

The Australian Government has a wider perspective and access to information about national interest risks that can guide universities' good practice. A joined-up and collaborative partnership approach between universities and government should be further developed, through which improved communications and timely information flows can be achieved. This could be facilitated by the Australian Government adopting a whole-of-government approach to how it engages and operates on managing risks relating to universities. On the university side – being a large organisation – we recognise the need to clarify roles, maintain communication and ensure our systems are rigorous and fit for the challenge.

A collaborative, transparent and mutually supportive partnership on foreign interference risks and responses is a crucial foundation for strengthening national security, while enabling the confident and responsible global engagement and vital research links so important to Australia.

For more information, please contact Professor Michael Wesley, Deputy Vice-Chancellor (International), [REDACTED]

Recommendations

Underpinning principles and values for managing foreign interference in the university sector

The Australian Government should adopt a collaborative partnership approach with universities to manage foreign interference through the following:

- **Adopt the UFIT model as an ongoing platform of bringing relevant agencies and universities together to co-design fit-for-purpose responses as required and provide advice and guidance to the sector.**
 - UFIT could be the standing forum, comprising senior university and cross-agency government representatives, through which timely, detailed, two-way information is supported to inform about risks, share information and best practice, and agree on mitigants.
 - UFIT could assist whole-of-government alignment on policy development and engagement with universities.
- **Interventions should build on existing arrangements where possible and complement the governance structures, integrity frameworks and operational systems typical in universities.**
 - Risk mitigation should seek to protect desired global engagement and international collaboration by Australian universities in view of the social, economic, research, and educational benefits these deliver.
 - Regulation relating to foreign interference should protect Australian research values, such as freedom of speech and academic freedom.
- **Interventions should be consistent, coherent and complementary across the suite of government regulatory regimes. New regulations:**
 - Should be subject to a robust, independent, regulatory impact statement to identify duplication and assess for whole-of-government complementarity.
 - Should adopt precise and targeted measures to provide certainty for universities and potential partners.
 - Manage sensitively commercial-in-confidence information under disclosure requirements to protect and encourage valuable global engagement and collaboration.
 - Be supported by an implementation Taskforce that provides, from government and regulators, clear and pragmatic guidance at the earliest opportunity on how to understand, apply and meet new legislated requirements of compliance, risk mitigation and reporting.
- **Collaboration, cooperation and continual improvement would be facilitated by:**
 - Clarification from Australian Government agencies on areas of responsibility, accountabilities and practical resources available to universities for security-related queries and scenarios.
 - Provision of real-time information exchange with key and trusted personnel.
 - Intelligence-based guidance from the Australian Government, including which tools should be used for assessments, to assist universities' decision-making about national security considerations in foreign engagement.
 - A mutual approach to updating and sharing monitoring and assurance reports.

Responses to the Terms of Reference

A) Foreign interference and Australian universities: context and characteristics

Global engagement and geopolitical dimensions

The University of Melbourne is a proudly global enterprise, reflected in the scope and scale of its research networks, student mobility programs and its global alumni network. Its current Strategic Plan, *Advancing Melbourne 2030*, outlines the University's strengths in collaborating with research, innovation and education powerhouses across Asia and the Pacific, Europe and North America. The University has developed engagement plans for three countries – India, Indonesia and China – for 2020-2024. These plans, which are all publicly accessible, articulate the University's teaching and research relationships and collaborations and our commitment to building these in the national interest over the long term.

The University's educational excellence and ethos is shaped by a substantial cohort of international students and staff (coming from over 150 countries); renowned globally-focused institutes and world-leading research centres (such as Asialink, the Nossal Institute for Global Health, the Australia India Institute, the Peter Doherty Institute for Infection and Immunity); strong student participation in international study and exchange programs (including the New Colombo Plan); and formal partnerships for research or student mobility with over 250 institutions worldwide. **Appendices A and B** outline the University's global engagement and research impact in more detail.

This openness to the world, with an emphasis on partnerships within Asia and the Indo-Pacific, is an uncontroversial position that aligns closely with Australian Government priorities, including those articulated in the 2017 *Foreign Policy White Paper*. The University, like the Australian Government, prudently manages its global engagement to ensure that openness is strategic, selective and secure. However, the recent period has seen a recalibration of some aspects of Australia's foreign relations to reflect changing geopolitical dynamics, heightened trade tensions, and increasingly, open clashes of interests and values between Australia and some of its strategic partners.

In the current environment, it is clear that responsible global engagement within the university sector requires a high level of information, awareness and preparedness. The University of Melbourne is aware of the real and present risk of foreign interference. It is actively reinforcing the autonomy and security of its operations and engagements in Australia and globally while advancing the benefits of international engagement.

Soft diplomacy and the value of international engagement

Efforts by universities to safeguard, while also maintaining, productive global connections, including with key Asian partners, will constitute a valuable goodwill-based connection and pipeline for engagement in years to come. The University's global engagement is a dynamic source of people-to-people and institutional linkages, with longevity, knowledge and insight that goes well beyond the capacity of national governments. Alumni of the University of

Melbourne and other Australian universities go on to become government, business and cultural leaders within our region. Ensuring a multiplicity of voices and relationships is a key plank of soft diplomacy and serves Australia's long-term national interest by furthering our capacity to engage respectfully and work with our region.

Australia is an outward-looking nation, with a record of achievement as a trader of goods, services and education exchange. Through historic signature initiatives like the Colombo Plan and New Colombo Plan, Australia has sought to exert influence, forge relationships and drive prosperity in our region for generations. Consistent with this, the University of Melbourne hosts or participates in a number of specialised institutes for engagement with specific countries or regions. These centres contribute unique connections and expertise with key countries in Australia's region.

- **The Australia India Institute (Aii)**, established in 2008 and hosted by the University, is the premier Australian centre dedicated to the study of India and the bilateral relationship. Funded by the Australian Government and the University, with others, Aii specialises in research and engagement in areas including education, health, equity, infrastructure, and governance. Aii also hosts the annual Australia India Leadership Dialogue, a pre-eminent bilateral forum for informal diplomacy, funded by Visy Industries.
- **The Asia Institute**, based in the Faculty of Arts, is the University's key centre for studies in Asian languages, cultures and societies, as well as a catalyst for community and business sector engagement and cultural exchange.
- The University of Melbourne is a partner in the **Australia-Indonesia Centre** based at Monash University, a bilateral collaborative research initiative established in 2014 by governments, leading universities, and industry.
- **Asialink**, founded in 1990, is hosted by the University and serves as one of Australia's leading centres for engagement with Asia. Supported by a combination of university, government, philanthropic and fee-for-service funds, Asialink develops insights, capabilities, and connections through programs and engagement in the arts, business, diplomacy and education. Asialink Business plays a unique role in building Asia-capability and supporting Australian businesses to forge relationships, enter and negotiate Asian markets.
- **The Centre for Contemporary China Studies** in the Faculty of Arts is a hub for research-based information on contemporary China, Chinese economies and Chinese society. It is one of the oldest and largest multidisciplinary Chinese Studies programs in Australia and Australasia.
- **The Asian Law Centre** in the Melbourne Law School was founded in 1985 to develop understanding of Asian law and promote interest in Australian legal systems (and others) within Australia's region.

The cross-section of experience amongst national parliamentarians illustrates the value of two-way international education and global mobility for building Australian connections, skillsets

and leadership in a broader sense, across a wide field of endeavour. Many of Australia's leaders, including two-fifths (9 of 23) of the current Federal Ministry, studied overseas as international students. In our home state, all the Victorian Liberals in the Federal Cabinet were international students. Nearly half of the members of the Parliamentary Joint Committee on Intelligence and Security have links with overseas universities, ranging from degrees to international executive education to visiting fellowships. This breadth of international experience serves Australia's interests.

The University recognises that the Australian Government is not suggesting that valuable global engagement should cease; but rather, is proposing that the known and emerging risks should be effectively managed. The University concurs and stands ready to collaborate in a two-way, respectful working relationship between universities and government, where collective action is proportionate to the risks being addressed.

Collaboration and progress on UFIT Guidelines

Australian universities have demonstrated an ability to mobilise and work with the Australian Government and its agencies to efficiently improve overall sector preparedness. In 2019, the Australian Government (through the Department of Education and Training) brought 13 universities and ten Government agencies together to collaborate on the University Foreign Interference Taskforce (UFIT). The University of Melbourne was supportive and engaged in this process, including by providing experts to several of the working groups.

In November 2019, the resulting *UFIT Guidelines* were published with endorsement by the sector – an output that has been recognised as world-leading, both in terms of the content and the collaborative approach between universities and government. The process was cooperative and trust-based, combining the breadth and experience of the research sector with the specialist intelligence and expertise of Government and security agencies. The *UFIT Guidelines* take a principles-based and proportionate approach aimed at balancing national security concerns with research imperatives and benefits.

As a case study in policy development, the *UFIT Guidelines* process serves as a good model for problem solving, effect change and raise awareness and preparedness across the sector. It served as an important cross-sectoral, cross-government confidence building measure. As discussed in more detail in Section D, Australia's *UFIT Guidelines* and sectoral collaboration has occurred efficiently and arguably at pace with, or ahead of, similar efforts in peer countries including the United States and United Kingdom.

As such, the *UFIT Guidelines* should form the foundation on which other regulation and interventions are built. UFIT, as a process, should be a model for whole-of-government engagement with the sector. As a specialist team within government, the University Foreign Interference Taskforce should continue to actively engage with the sector, including the sharing of information and best practice, providing updates on developments that may require university response, and building mutual respect and understanding.

Throughout 2020, the University of Melbourne has worked to continuously improve its implementation of the suite of enhanced national security measures set out by the *UFIT Guidelines*. This includes the establishment of a university-wide Foreign Interference Working

Group, and other senior leadership working groups, to oversee compliance and ongoing implementation work plans. Awareness of the issues and approaches recommended in the *UFIT Guidelines* at an appropriately senior level of the institution has been instrumental in establishing a risk-literate culture on foreign interference matters, and embedding appropriate risk mitigation into institutional decision-making. This submission elaborates on the University's activities and planning in more detail in Section B.

Sector co-operation and activity on countering foreign interference

The university sector is working together across various workstreams to improve security against foreign interference. For this reason, any Australian Government interventions that are recommended out of this committee inquiry should be co-designed with the university sector, bringing the experience and perspectives of the higher education sector into solutions and extending the proven collaboration model developed through *UFIT*.

Within the Group of Eight (of which the University of Melbourne is a member), cross-university leadership groups are proving effective and catalysing forums for developing best practice and exchanging information (e.g. Vice-Chancellors and Deputy Vice-Chancellors; General Counsels; Research Directors; Ethics and Integrity Directors; and others). Across the sector there are also specialised working groups that draw together subject matter experts in areas such as sanctions and export controls, which are already governed by existing legislation.

This record of collaboration and development demonstrates the whole of sector benefits that flow from sharing information on systematic implementation and risk management. Ultimately, the wide experience and diversity of the university sector is an advantage for developing and implementing best practice. This is reflected in the goodwill-based collaboration seen already, such as:

- Reciprocal commitments to sharing of information, including in relation to information technology (IT) threats and cybersecurity experiences, as discussed in more detail below.
- Active discussions about pooling resources to develop and update staff training materials.
- Sharing of foreign interference mechanisms such as different universities' approach to managing disclosures of interests or securing IT systems.
- Sharing of *UFIT* Implementation Work Plans and the structure of staff awareness and training programs.

The implementation of the recently passed *Australia's Foreign Relations (State and Territory Arrangements) Bill 2020 (the Foreign Relations Bill)*, would benefit from a collaborative approach to advise universities on compliance and build up a knowledge base.

Recommendation

- **Adopt the *UFIT* model as an ongoing platform of bringing relevant agencies and universities together to co-design fit-for-purpose responses as required and provide advice and guidance to the sector.**

- UFIT could be the standing forum, comprising senior university and cross-agency government representatives, through which timely, detailed, two-way information is supported to inform about risks, share information and best practice, and agree on mitigants.
- UFIT could assist whole-of-government alignment on policy development and engagement with universities.

The importance of global research, education and engagement

As a research-intensive and comprehensive university, the University of Melbourne is internationally connected across education and research, drawing on relationships built over many years that span the globe in the pursuit of the world's best collaborators. These relationships are delivering approximately 2000 active arrangements across 57 countries, providing valuable educational experiences for our students and Australia with world-class research that is translated into new discoveries in medicine, public health, manufacturing, engineering, agriculture and more.

In the long tradition of increasing the wellbeing and prosperity of the nation through international engagement, the University's partnerships are carefully managed to protect national interests and deliver sovereign capabilities that would otherwise be out of reach for Australia. Substantial and irreplaceable national benefits thus accrue from our international engagements that have served the nation well since Federation.

The University engages with global organisations such as the Bill and Melinda Gates Foundation, the Wellcome Trust, Atlantic Philanthropies and the World Health Organization in the investigation, dissemination and application of research which addresses some of the most pressing global problems. These partnerships underpin significant projects to help humanity, such as funding to trial a coronavirus vaccine amongst healthcare workers (Gates Foundation); grants to understand and treat malaria in pregnant women (Wellcome Trust); and support for social change leadership to reduce inequality and discrimination against Indigenous and other disadvantaged populations in Australia and the Pacific region (Atlantic Philanthropies).

Australia's sovereign capability, protected by its national security apparatus, is strengthened by a highly proficient and competitive research and development sector. The case study of the Peter Doherty Institute for Infection and Immunity on the following page is an illustration of the fundamental importance of foreign collaboration, resources and funding in biomedical research. Success here has particular contemporary significance to Australian, and global, public health. Other examples demonstrating the importance of international collaboration include the following:

- Some research depends on infrastructures and facilities that are innately global due to their massive scale, such as CERN's Large Hadron Collider in Switzerland and the Square Kilometre Array project in South Africa and Australia. These types of projects bring together the world's finest scientists, engineers and policy makers to undertake transformational science on a scale not achievable by one institution, organisation or country alone.

- In some areas of research, there are only a few laboratories or appropriate facilities in existence globally (e.g. CERN); as such it would not be feasible for even the United States or China to undertake all of its research within national borders, let alone Australia. Australian researchers depend on collaboration to be able to do such work.
- Some important research is fundamentally designed around global collaboration. Research that depends on data volume often requires data far beyond country borders, such as that for rare diseases. The Stawell Underground Physics Laboratory in Victoria – the first in the southern hemisphere and a crucial new site of global research into dark matter – is feasible because it is a complement and directly linked to work being undertaken in the northern hemisphere. Other research (e.g. on disease progression) is useful due to its comparative findings across populations or jurisdictions.
- International networks of universities can provide access to a broader range of expertise and facilities than is available nationally. These connections and knowledge reservoirs serve as a form of insurance for cutting-edge research in Australia, ensuring that when a need arises, core capabilities will remain accessible even when they are likely to exist externally.

Recommendation:

- **Interventions should build on existing arrangements where possible and complement the governance structures, integrity frameworks and operational systems typical in universities.**
 - Risk mitigation should seek to protect desired global engagement and international collaboration by Australian universities in view of the social, economic, research, and educational benefits these deliver.
 - Regulation relating to foreign interference should protect Australian research values, such as freedom of speech and academic freedom.

Case Study 1: The Peter Doherty Institute for Infection and Immunity at the global frontline of COVID-19

The Peter Doherty Institute for Infection and Immunity (the Doherty Institute) – a joint venture between the University of Melbourne and The Royal Melbourne Hospital – is a powerhouse of education, research and public health development and a global leader of the response to COVID-19.

Role in the COVID-19 response

When the pandemic started, the Doherty Institute directed its resources and capabilities almost solely towards understanding and responding to the disease. The first diagnostic test for the virus in Australia was established at the Doherty Institute before the technology was transferred to labs across the country and regionally. The Doherty Institute was also the first to grow the live virus outside of China, an important step for vaccine development and validation. This

technology was distributed widely around the world unconditionally in support of the global effort to create vaccines and treatments.

A significant program of work has studied potential antiviral drugs for treatment of COVID-19, mapping the immune response to the virus and supporting vaccine development. Pandemic modelling by Doherty scientists informed both national and international government policy on travel restrictions, social distancing and quarantine.

In the latter half of 2020, the Doherty Institute, working with the Victorian Government, led research and piloting of saliva testing methods for detection of COVID-19, including a workplace testing program. The early results of this ongoing research have delivered a better understanding of the logistics of continuous testing in higher-risk workplaces. The findings have also reassured policy-makers and scientists that saliva testing is a reliable equivalent test to throat and nasal swabbing, and is easier and more comfortable to take, reducing risks to health care workers who administer the test and consuming less PPE and swabs.

The Doherty Institute's crucial international collaborations

Most of the Doherty Institute's research is based on international collaborations, reflecting contemporary norms in science. These partnerships are a mixture of funding, knowledge, experience, skills, equipment, access to pathogens, access to animal models and access to different clinical cohorts – a crucial combination of resources and inputs that cannot be replicated within Australia.

- International collaboration was necessary for Australia's vaccine development, as Australia currently does not have the capacity to undertake vaccine candidate testing on animals like hamsters (as they are a banned species). As such, the Doherty Institute collaborates with Hong Kong University to do this work, supported by the National Foundation for Australia-China Relations (within the Department of Foreign Affairs and Trade). This work includes access to technology unavailable in Australia, but also a two-way exchange of knowledge.
- The Doherty Institute has commercial contracts with Colorado State University to undertake this crucial work using animal models.
- The Doherty Institute's work on an HIV cure is funded by the National Institutes of Health in the US (\$1 million) and is a partnership with the University of California San Francisco and others. HIV cure clinical trials are conducted with global partners in countries such as Thailand. The American Foundation for Aids Research, also provides \$1 million.
- The Doherty Institute's influenza work is done in collaboration with Fudan University, utilising scientific expertise at both sites and the large clinical cohorts available in China.
- The Doherty Institute's malaria research is done in collaboration with regional partners, as malaria is no longer found in Australia but has a tremendous impact in our region.
- The Doherty Institute is also the secretariat for the International Coalition for the Elimination of Hepatitis B, working with overseas partners including France, the US and

China. Asia has some of the highest rates of Hepatitis B and is a critical partner in the search for a cure.

International funding for Doherty Institute work

A considerable portion of the Doherty Institute's funding comes from foreign sources. Funding and partnership agreements support the work of the Institute but also create an environment for ideas exchange, collaboration and peer-to-peer relationships amongst globally leading medical researchers. For instance, the Doherty Institute participates in or receives:

- Matched funding for joint PhD positions with overseas universities including Bonn (Germany) and Fudan (China), and matched funding for joint roles with Institut Pasteur (France).
- Donations or competitive grant funding from the Wellcome Trust (UK), National Institutes of Health (US), Gates Foundation (US), GFATM (Global Fund to Fight Aids, Tuberculosis and Malaria) (US) and other global foundations.

Further examples of overseas funding to the Doherty are included below. Even if the Australian Government were in a position to fund this research (which it presently does not) international collaborations are critical to Australia's science sector. Beyond funding, the exchange of ideas, skills, materials and knowledge are essential to keep Australian scientists at the forefront of international research.

- Jack Ma Foundation donated \$3.2 million towards vaccine development, representing about 50% of vaccine development funds currently available to the Doherty Institute.
- a2 Milk, New Zealand-based, donated \$500,000 towards basic COVID-19 research at a very early point in February 2020.
- John Martin, US based, donated \$500,000 to a virology fellowship looking at workforce development in virology. Ray Shanazi, US based, donated \$100,000, and Morningside Foundation, Hong Kong based, donated \$750,000 to the same.
- The Fleming Fund, UK based, provides \$1-2 million for fellowships in capacity building across the Indo Pacific region.
- Pharmaceutical companies, including ViiV, Gilead, Roche and GSK, make significant contributions to programs in Hepatitis B, HIV cure and influenza antiviral development.

B) The University of Melbourne's awareness of foreign interference, undisclosed foreign influence, data theft and espionage, and its capacity to identify and respond to these threats

The University recognises that theoretically there is a degree of foreign interference risk in everything we do – teaching and learning, research, engagement, the activities of professional and academic staff – and that risk is not only external but also could be internal. The University recognises that risk may be present or may emerge in either established or new relationships,

to varying extents and in different forms. The following sections outline the architecture of the University's capacity to identify and respond to complex and dynamic foreign interference risks, and how under its program of continuous improvement it has been strengthening its systems across the institution.

Governance and culture

Ensuring resilience against foreign interference is recognised by the University as a continuing priority. Integration of these risks into existing reporting and governance structures enables oversight at the most senior levels of the institution. A range of educative initiatives further develops a culture of awareness and uplifts risk literacy. Escalation pathways and subject matter expertise to support the University community to identify and mitigate risks appropriately form part of a risk-aware culture. Commitment to continuous improvement across all domains, supported by processes and policy, is a key aspect of ensuring that the University operates in a manner that is responsive to new risks as they emerge and best practice approaches.

Compliance with Australian laws and regulations

In accordance with Australian laws and regulations, the University is aware, engaged and proactive in mitigating foreign interference risks. It has well-established mechanisms for due diligence, integrity and compliance, risk identification and escalation protocols, and a record of communicating with Australian Government departments and agencies on a multitude of compliance regimes and on issues of concern or uncertainty.

An extensive suite of national interest legislation and various compliance requirements currently exist. Universities must comply with the following when dealing with foreign entities:

- *Autonomous Sanctions Act 2011 (Cth)*
- *Autonomous Sanctions Regulations 2011 (Cth)*
- *Foreign Influence Transparency Scheme Act 2018 (Cth)*
- *Defence Trade Controls Act 2012 (Cth)*
- *Defence Trade Controls Regulation 2013 (Cth)*
- *Export Control Act 2020 (Cth)*
- *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018.*

Most recently, the passage of *Australia's Foreign Relations Bill* through Federal Parliament, which seeks to align State, Territory and public universities' foreign relations or arrangements with national foreign policy, will require further compliance developments.

The University's defence and dual-use research capabilities carry elevated risks relating to foreign interference threats. Some University of Melbourne research also draws on microbiological agents and toxins that are subject to biosecurity controls. The risks at this end of the scale are known and comprehensively managed with dedicated staff roles and established systems. The University has built up considerable experience in compliance and risk mitigation in its own context.

With regard to undisclosed foreign influence, the University is committed to meeting its obligations under the *FITS Act*, the registration scheme under which organisations and some individuals must register certain activities conducted on behalf of foreign principals. For illustrative purposes, a detailed case study of risk management arrangements for the Confucius Institute at Melbourne is included below.

The University is implementing new standards and dedicated officer roles for physical and cybersecurity as required by the Defence Science and Technology Group (through the Defence Industry Security Program). The Government has also established a unit within TEQSA, the higher education regulator, to work collaboratively with government bodies that have primary responsibility for other integrity threats relevant to higher education, such as cybersecurity, foreign interference and research integrity.

The University is following the progress of Federal Government bills under consideration:

- proposed changes to the *Security of Critical Infrastructure Act 2018*, which will include universities in adopting measures to protect critical national infrastructure.
- the *Higher Education Support Amendment (Freedom of Speech) Bill 2020*, which seeks to redefine and strengthen legislative protections for academic freedom and freedom of speech.

In addition to the above legislative regimes, publicly-funded research councils have their own integrity measures and disclosure requirements. All research undertaken at the University is governed by established procedures for ethical review and compliance following the *National Statement on Ethical Conduct in Human Research*, and research integrity is managed according to the *Australian Code for the Responsible Conduct of Research*. All University members – including graduate researchers and honorary staff – must also adhere to a number of University policies and processes that align with national codes and frameworks (see **Appendix D** for more details of compliance and policy overlay).

The ARC's recently amended *Conflict of Interest and Confidentiality Policy* is a further example of requirements for transparency and full disclosure in relation to the international activity of academic staff. The changes made by the ARC in September 2020 clarify the types of personal interests that Australian researchers must identify and disclose when submitting grant applications for funding from the ARC.

However, it is not clear whether the data collected through the ARC will form any part of the formal ARC review and assessment of the application. The ARC has advised universities that the inclusion of the questions is designed to help Administering Organisations (i.e. the University) comply with the *FITS Act*. However, as the University has its own *FITS Act* compliance regime, there is a risk of duplication and potential uncertainty emerging as government entities seek to impose more layers of risk mitigation.

A multitude of regulation can also cause unhelpful and counter-productive overlap. This may be evident in the current process for export permit applications, which controls the technologies that the University can make available internationally. The University understands that Defence (the permit issuer) consults with DFAT on foreign policy alignment as part of its approval processes, suggesting that there may be some scope to rationalise the regulation of

international research arrangements under the *Australia's Foreign Relations Bill*. Duplication can create its own risks, especially if it dilutes focus away from the most sensitive activity, such as that regulated by Defence Trade Controls.

From the University's perspective, the more compliance requirements that exist, the more diluted resources become and the greater the risk of inconsistency and loss of systemic processes and oversight. It is important that regulation is calibrated to appropriately control high-risk activity, but not to create an unnecessary over-regulation of low-risk activity. This creates a resource burden on both universities and regulators without a useful dividend. As the subsequent sections document, the University takes seriously the challenge of foreign interference and is reviewing and improving its risk mitigation.

Capacity to respond to threats: due diligence and UFIT implementation

The *UFIT Guidelines* identify due diligence as a key strategy to embed foreign interference considerations into business as usual activities. Due diligence forms a long-standing part of institutional decision-making, but screening has been strengthened to allow for enhanced due diligence processes when risk factors identified in the *UFIT Guidelines* are flagged. Pathways for escalated decision-making are in place, for example, to the University's Research Due Diligence Advisory Group, to ensure that institutional decision-making takes the *UFIT Guidelines* into account.

Due to foreign interference risks and the additional reputational risk evident in the external operating environment, the University has established additional working groups with specific accountabilities. The newly-established Foreign Interference Working Group is focused on driving greater awareness, visibility and oversight of foreign interference risks. In particular, the Working Group has oversight of the implementation of the *UFIT Guidelines*.

The University is continuously improving its internal processes and progressing a staged UFIT Action and Implementation Plan. This work includes:

- **Outreach and training programs** to University academics and staff to elevate awareness of the *FITS Act* and its application across all domains of the University.
- **Upskilling of relevant staff**, including in Legal Services, to assist in identifying potential foreign interference risks in contracts, and where necessary, working with the contract owner to ensure compliance with the *FITS Act*.
- Launch of a ***FITS Act* online training module** that is accessible to all staff, and mandatory for University members working in research or philanthropy.
- **Strengthened risk management framework**, including compliance management and escalation protocols for decision-making and oversight of higher risk research proposals.
- Development of a **communications program** to inform and train staff about the *UFIT Guidelines* and related legislation and obligations.
- Integration of information on foreign interference risks into **induction programs** for new staff, commencing graduate researchers and their supervisors.

- Refinement of systems that **capture conflicts of interest**, including those pertaining to foreign arrangements and potential risks.
- Enhanced due diligence processes and **screening of potential partners**.
- Refinement of internal **registration of international partnerships and databases** about partnerships to streamline oversight across the institution.
- Assessment and improvement of University **cyber and physical security** and oversight, including roll-out of a training module on cybersecurity that is mandatory for all staff and graduate researchers.
- Enhancement of **risk assessment and due diligence for gifts**, including templates and tools to ensure gift acceptance only occurs with sufficient knowledge of the donor and purpose, and consistency with University policies and State/Federal laws in Australia.
- Development of plain-English resources describing foreign interference concerns and **raising awareness amongst staff and students**, which are circulated through student clubs and societies during Orientation.
- Provision of advice to students on how to **responsibly conduct political activities and statements on campus** through the Geopolitical Risk Advisory Group.
- Improvements to University **international travel policy**, procedure, process, practice and supports related to both staff and student travel.

Case Study 2: Risk management and the Confucius Institute at the University of Melbourne

As with 13 Australian universities, and 541 globally in 162 countries, the University of Melbourne hosts a Confucius Institute (CI).

The University's involvement in the Confucius Institute has delivered positive outcomes including:

- High-quality provision of public-access Chinese language and cultural programs;
- Training and advice, enabling the University to effectively engage with Chinese stakeholders both in Australia and Greater China;
- A valuable ongoing relationship with Nanjing University, one of China's top tier universities; and
- A strong program of cultural and linguistic events for the wider community and valuable engagement with the Chinese-Australian community.

History

In 2006, the University signed a Memorandum of Understanding (MOU) with the global Confucius Centre Headquarters (the "Hanban", a division of the Chinese Ministry of Education) for the establishment and operation of a Confucius Institute (CI or "the

Institute”) in partnership with Nanjing University. The MOUs and then agreements with the Hanban and Nanjing University were renewed over several years, most recently in 2019 to reflect new obligations of the University of Melbourne including under the *Foreign Influence Transparency Scheme Act 2018 (FITS Act)*.

In 2020, the Chinese government reorganised the management of Confucius Institutes globally, passing responsibility from the Hanban to the Centre for Language Education and Cooperation (CLEC) and the Chinese International Education Foundation (Foundation) as well as expanding the role played by the university partner. The University has recently concluded successor agreements governing the operation of our CI with those organisations and updated our agreement with Nanjing University. The University has shared its reviews of its CI and the agreements underpinning it with Federal Government agencies, including Attorney-General’s Department, Department of Home Affairs, Department of Foreign Affairs and Department of Prime Minister & Cabinet.

Governance

At Melbourne, there are clear boundaries between the University’s academic and research activities and the current activities of the Confucius Institute. There is effective day-to-day management of the CI by the University (Deputy Vice-Chancellor, International; the Assistant Deputy Vice-Chancellor International (China); and the CEO of Asialink).

A University Executive Management Committee which provides oversight of the CI, includes representatives of three faculties and meets biannually. A Joint Management Committee with representation from the University and Nanjing University meets annually to discuss broad directions for the Institute. Limited funding is provided by the University of Melbourne and Nanjing University, with equivalent, reciprocal annual grants.

The CI complies with Australian laws, education quality standards and principles of academic freedom. The agreements and management of the CI at Melbourne are premised on the need for the University to ensure:

- The University’s institutional autonomy and control of curriculum and standards in the University of Melbourne CI;
- Transparency of all CI agreements and programs, particularly to government agencies with regulatory oversight under the FITS Act and other Commonwealth legislation;
- Control by the University over finances, decision-making, programs and their evaluation, and staff activities; and
- Full compliance with all relevant Australian Government legislation, policy and procedures.

Taken together, these measures give us a high degree of confidence that the CI at Melbourne operates in a way that is both appropriate and delivers value to the University and our community.

The *FITS Act*

When the *FITS Act* came into force in December 2018, the agreements between the University and Hanban, and with the Nanjing University, gave rise to relationships that could *prima facie* appear as potentially registrable under the Scheme.

Subsequently in 2019, two separate reviews looked at the activities of the CI and applicability of the *FITS Act*. This included an internal analysis conducted by the University and the provision of formal external legal advice. Both reviews found that the activities of the CI at Melbourne do not fall within the type of activities that are registerable under the *FITS Act*. In mid-2019, following briefings on the University's risk assessment, due diligence and compliance with the *FITS Act*, that assessment was confirmed by relevant Australian Government agencies.

Risk Management

In addition to ensuring full compliance with the *FITS Act*, the University has established a comprehensive approach to monitoring, managing and evaluating CI activities and ensuring ongoing legal compliance and addressing foreign interference considerations.

Ongoing risk management measures taken by the University include the following:

- All CI personnel have received training on the *FITS Act* obligations and have been provided with guidance for consistently assessing whether CI activities may require registration;
- All CI employees must comply with University policies, including the Code of Conduct and the Academic Freedom and Freedom of Speech policies, and all Australian Government legislation and policies at all times;
- The University has commissioned independent reviews of Chinese language teaching materials used by the CI which found the materials were balanced and appropriate for an apolitical language course;
- The University conducts training on the *FITS Act* for secondary schools participating in the Confucius Classroom program attended by principals, heads of Chinese teaching and teaching assistants provided through Hanban;
- The University hosts regular Confucius Institute Network meetings to share best practice around the *FITS Act*. These have been attended in some cases by relevant Australian government officials;
- The University has undertaken to (and does) provide the terms of its agreements with CI partners to any interested party on request; and
- The University Executive Management Committee with oversight of the CI undertakes a biannual comprehensive risk review of the CI and its operations.

Capacity to respond to threats: research and associated governance

Research ethics and integrity

Separate to foreign interference considerations, University research occurs in an environment shaped by commitment to core values and to upholding practices of research integrity and accountability. All research at the University, including research with external parties, must uphold the 'Research Principles' documented in the *Research at Melbourne Strategy*. These principles bring together key aspirations, such as the long-term community benefit derived from the research, as well as formal policy commitments, such as the endorsement of academic freedom, ethical standards and research integrity.

These Research Principles are supplemented by the following 'Key Principles and Due Diligence Practices', which are in turn implemented by a mix of policy-based protocols, disclosure processes, supervision and committee oversight, due diligence escalation and decision-making pathways, and staff education:

1. The conduct of research is governed by respect for the principle and exercise of academic freedom.
2. Research is undertaken according to the highest standards of research ethics and integrity, governed by legislative, regulatory and institutional frameworks.
3. Conflict of interest is addressed through a transparent process for identifying and managing any arrangements that might otherwise compromise, or appear to compromise, the independence of research.
4. Research funding sources are disclosed in order to promote accountability, openness and clarity of research purposes.
5. Due diligence processes are engaged from the outset of prospective research collaboration with external partners.

The University balances potential benefits and harms of research with reference to its values and community standards. Its policy and practices reflect a high-risk threshold for intellectual curiosity and exploratory research and a low-risk threshold for research that causes harm to humans, animals, or the environment or jeopardises the values and reputation of the University.

The Office of Research Ethics and Integrity (OREI) is the University's main point of contact for issues relating to animal welfare, animal and human ethics, research integrity, research misconduct, gene technology, biosafety, biosecurity, and export controls. Specialist roles within OREI oversee the University's framework for managing export controls and sanctions and ensure that the full circumstances of any proposed research funding are understood before being accepted.

Governance of sensitive research

In 2018, the University undertook a program of work to develop a principles-based framework to guide decisions about undertaking research with external parties. This included a decision-

making pathway for determining when particular research and research partnerships present potential risks to the University's research values and reputation and/or jeopardise the integrity and independence of its research.

The following high-level outline of decision-making on external research partnerships at the University of Melbourne illustrates the practical architecture for oversight and risk management:

- The University has established a Research Due Diligence Advisory Group (RDDAG), a senior cross-institutional committee to provide review for research due diligence processes and risk, and to consider emerging and potential risks at sector and national level. Membership of the RDDAG has been extended to include a University Council member who also sits on the University's Gifts Committee to ensure oversight of due diligence on donations that may overlap with due diligence for research.
- Critically, RDDAG has brought together different areas of the University, such as Research and Advancement portfolios, to capture risk related processes and matters that might arise via a number of avenues so as to ensure a coordinated, whole-of-institution response.
- *RDDAG escalation protocol*: When a clear-cut decision on process review is not possible and/or if significant risks are identified, RDDAG refers the matter to the office of Deputy Vice-Chancellor Research for final determination on whether to proceed with particular external research partnerships or contracts.
- Decisions to initiate research partnerships and collaboration typically begin with researchers and Academic Divisions and include layers of consultation with specialist staff (such as Legal and Risk, Export Controls, Ethics Office) across the University.

Managing export controls, sanctions and biosecurity risk

The University has well-established processes to manage export controls, sanctions and biosecurity risk. These programs are resourced by dedicated subject matter experts and are subject to a cycle of continuous review and improvement. Given the diverse University context and devolved nature of operations, the programs feature regular outreach to the University community to raise awareness of issues and pathways for support, as well as screening mechanisms to detect relevant activity and offer advice to academic and professional staff as well as graduate researchers. Subject matter experts are in regular contact with the Department of Defence and DFAT. They also conduct:

- Monitoring of the external landscape for new developments.
- Preparation of training and education programs to inform and support staff to adhere to compliance requirements and other obligations.
- Data capture to identify trends as well as areas for targeted attention and improvement.
- Regular reporting to institutional management on risk and compliance activity.
- Appropriate review of detected non-compliance to understand root causes and improve overall system robustness.

Capacity to respond to threats: risk awareness and training amongst University members

The University has a responsibility to inform its members of risks and how to manage them. Experience of recent years across the sector reinforces the need to ensure all members of the University community are trained and cognisant of the requirement for due diligence and disclosure across all their work and engagement activities. The University is working to deepen and embed a risk aware mindset amongst its community to ensure that staff conduct and culture reflects an understanding of, and alertness to, potential foreign interference. The University leadership, working in concert with Faculty Deans and Heads of School, are facilitating this systemic enhancement, building on strong foundations that are already in place.

Refreshed training programs, supported by communications campaigns, are being launched to ensure that all University members are aware, reminded and encouraged to identify and disclose potential risks as part of their professional/scholarly mindset and practice. Other enhancements that support a risk aware culture include:

- The University's policy library includes a Freedom of Speech Policy to ensure freedom of teaching, learning, debate, criticism and knowledge in the University, including in the lecture theatre and tutorial room.
- The University's subject matter experts across research, export controls, research ethics and legal units provide specific advice on institutional processes and cases.
- The newly-established Researcher Development Unit provides advanced professional development to researchers, coordinates existing compliance training programs, including training programs to cover foreign interference risks.
- The University will continue partnering with the Australian Sanctions Office to offer annual DFAT-conducted sanctions training. Starting in 2020, the University has offered 'Know Your Partner' due diligence training. The University's Legal and Risk Unit is also developing a general compliance training module for new researchers that covers foreign influence, export controls and sanctions obligations.
- The University's conflict of interest and disclosure mechanisms are being updated to ensure that any conflicts of interest pertaining to foreign arrangements are appropriately understood, disclosed, documented and managed. This will assist in providing greater transparency and accountability, and strengthen visibility and our capacity to meet reporting requirements.
- A suite of other education programs is in place or in development include training relevant to foreign interference obligations and prevention, such as:
 - Foreign Influence Transparency Scheme Awareness
 - Research Integrity Online Training
 - Conflict of Interest – Research
 - Key Policies and Information for Academics

- Managing Information – Cybersecurity
- Appropriate Workplace Behaviour
- Biorisk – Biosafety Induction Online
- Casual Employees Compliance Training
- Defence Trade Controls
- Health and Safety – Roles & Responsibilities
- Key policies and Information for Academics
- Professional and Academic Staff Orientation and Induction
- Supervisor Graduate Research Online Course/Refresher.

Talent programs

Talent programs broadly take the form of academic awards that require a researcher to affiliate with the awarding institution, spend time overseas, and/or receive payment, access high-value information/data, or gain other professional benefits. Some talent programs provide funding for researchers to establish and run labs overseas. There are legitimate and well-recognised programs to support international academic exchange and the global research enterprise that could be described as talent programs.

Recent analyses of China's talent programs suggest that some programs operate through recruitment of international academics to expand China's strategic interests and generate access to valuable research and technologies. Concerns have been raised that talent programs may increase risks of covert foreign interference or may lead to the leakage or theft of Australian-funded research and intellectual property, and/or strategic technologies, including through circumventing export control restrictions. The University views these concerns seriously and is including talent recruitment as part of its program of continuous improvement of due diligence and risk management.

University sector peak bodies have conveyed the Australian Government's affirmation that talent programs can potentially encompass *both* legitimate and illicit research activity. Presently, there is no prohibition on talent program-based recruitment or activities through universities. As such, the University's approach on this is to: require disclosure under the institution's 'Outside work' policies and processes; assess instances on a case-by-case basis using enhanced due diligence; and, if approved, ensure that appropriate risk mitigation is applied to address any risks. Potential academic involvement in talent programs is reviewed by the University's Research Due Diligence Advisory Group, which advises the Deputy Vice-Chancellor (Research) with respect to decision-making and receives input from senior academics and managers.

Awards under talent programs are personal and are made to the individual researcher. As such, *Australia's Foreign Relations Bill* would not capture talent programs if the University is not a party to the arrangement, and the *FITS Act* would only apply if the award involves seeking to influence the Australian Government on behalf of a foreign principal.

Physical and cybersecurity

The University of Melbourne takes a risk-based approach to cybersecurity under the authority of the Chief Technology Officer and the Director of Cybersecurity. The University maintains a range of administrative, technical and physical procedures to protect all information stored in our environment. The University is committed to a proactive approach to security and privacy by anticipating and preventing invasive events before they occur, and embeds security considerations into the design and architecture of information technology systems and business processes.

The Chief Technology Officer is overseeing a 5-year program (currently in year 2) to uplift cybersecurity capability across the institution to prevent, detect, and respond to cyberthreats. Efforts to date have reduced vulnerability to cyberthreats while balancing a practical need for platforms that support academic autonomy and collaboration. We recognise the University, as a large organisation and a research and teaching institution, carries a unique and complex cybersecurity risk profile. Universities' cybersecurity must encapsulate national security and intellectual property protections while also providing flexibility and functionality to support the fundamentals of university teaching and research activity.

In line with the experience of tertiary education providers around the world, the University routinely encounters and defends against cybersecurity threats, including sophisticated attacks that cannot be attributed to any known threat actors. The University is cognisant of the fact that Advanced Persistent Threat actors regularly test the University's defences. The University's cybersecurity team, which has doubled in personnel in the last two years, is able to learn from the tactics, techniques and procedures of these attacks and absorb this information into its risk management approach. No institution is completely impervious to risk in the cybersecurity space – but a range of steps can be taken to mitigate risk to a satisfactory degree. The University is advanced on this process of continuous risk mitigation and improvement in line with the *UFIT Guidelines* (as a minimum benchmark).

The University's cybersecurity framework, which has been effective against significant attack to this point, relies on components such as awareness, prevention, detection, rapid response and recovery. In practical terms, these components are illustrated by the following examples:

- All staff at the university receive an automatic notice when an email is received from an external source that is not in a 'safe sender' list, which heightens day-to-day staff awareness of email-borne risk and has dramatically reduced the impact of phishing or malware attempts.
- The University deploys a range of NextGen firewalls and in the past 12 months has rolled out multifactor authentication (MFA) for all staff accounts. Student account MFA will be rolled out in 2021.
- Specific and latest technology tools have been implemented to assist with detection and containment, supported by standing arrangements with external third parties with specialist breach containment capability.

- In line with the *UFIT Guidelines*, the University is currently running a threat modelling exercise with the assistance of an external cybersecurity consultancy. This will not only provide a better understanding of the threats the University faces, but will also generate a controls library that will be mapped to an industry standard framework (NIST). This project will additionally generate a list of risks, associated threats, and clarify the university's effectiveness of response, all leading to a stronger cybersecurity ecosystem.
- In 2021, the University is significantly uplifting its protections by introducing an Endpoint Detection and Response (EDR) capability into its IT environment. This will enhance the Cybersecurity team's ability to rapidly respond to threats even in remotely located University assets. It will be augmented by consuming a commercial threat intelligence feed to identify TTPs for advanced threat actors and risk conditions. In addition, a proactive threat hunting program will also be introduced to provide additional visibility into the environment.
- Overall, the University is approaching cybersecurity as a human issue (backed by technological tools), requiring higher cyber-threat awareness across all its members and reinforcement of a positive security culture.

In 2020 the University, which has biomedical research centres working on globally significant testing of COVID-19 vaccines, has been particularly engaged with the Australian Cyber Security Centre (ACSS) on protecting its critical research infrastructure. This has included collaborating with the ACSC to run a Cyber Hygiene Improvement Programs (CHIPs) scan to provide the University with information for the purpose of visibility, analysis and risk management.

As a global and research-intensive institution, the University's cybersecurity framework is sophisticated (see further details at **Appendix C**). As a publicly-funded university – not a defence research facility – the University is maintaining a balanced and secure system that is appropriately functional for its diverse users and usages (in global research, teaching and learning, and university operations) while not open to compromise.

Senior leaders of the cybersecurity team participate in Victorian and Australian communities of practice to contribute to the overall preparedness of the sector. IT managers and cybersecurity leaders at the University participate with the ACSC, other parts of the Australian Signals Directorate and colleagues across the sector, including sharing the latest information and reports on potential threats.

C) Australian Government role: coordination, partnership and advice

Leading a coordinated whole-of-government response

This submission has outlined the University's position that foreign influence (undisclosed), foreign interference, espionage and theft are recognised risks that can be managed effectively through strengthened preparedness supported by constructive partnership with government and key agencies. Future Australian Government interventions that seek to impose greater scrutiny of, and security in, universities should be proportionate to the risk and balanced against the vast majority of international research and engagements that deliver deep value to Australian society.

The University recommends the Australian Government approach the issue of foreign interference risk at universities through a coordinated, whole-of-government lens. As outlined above, there are multiple legal regimes covering foreign interference, involving regulation across several different departments, which creates the risk of overlap and duplication, confusion and different and/or conflicting standards of decision-making and outcomes. Genuine vigilance requires as much goodwill as it does black letter law.

The University of Melbourne – institutionally and across its different domains – already engages closely with Government departments and agencies on security policy and practical issues. For example:

- The University's International portfolio is regularly in touch with the Department of Home Affairs and Attorney-General's Department with regard to global partnerships and engagement.
- The University's specialised Office of Research Ethics and Integrity engages with Defence Export Controls in the Department of Defence, the Sanctions Office in the Department of Foreign Affairs and Trade, and the Department of Agriculture on matters related to biosecurity and technology development.
- The University regularly briefs and seeks advice from the Department of Education and Training on matters including security and policy.
- Operationally, senior leaders of the University have institutional relationships with ASIO, Australian Signals Directorate and the ACSC as needed. On related matters the University also engages with the Victorian Government, and to a lesser extent, the City of Melbourne.

The above examples demonstrate the extent to which the University of Melbourne staff are working collaboratively and appropriately with government to reduce foreign interference risk and maintain security safeguards.

The Australian Government has Australian interests as its fundamental concern, and many parts of the public service are specialist in the field of national security in a way that no university can replicate. The expert capability and real-time intelligence and expertise of organisations such as DFAT or ASIO stands as an important resource for universities. In addition to strategic leadership, there are a number of crucial roles for the Australian Government that can significantly assist universities to manage risk.

A coordinated, whole-of-government approach would enable clarification of responsibilities and accountabilities across departments and agencies, which would improve practical communications and proper direction of day-to-day queries from universities to government about security concerns. Linked to this, the sector would benefit from clarification of the extent to which universities are able to leverage government assistance in different areas.

For instance, there may be support and resourcing available to universities in areas such as strategic foreign relations, sanctions compliance and geopolitical developments. To ensure a greater alignment between universities and government on global engagement and risk management, clarified roles and resources would be of high utility.

Provision of national security advice and intelligence

Where appropriate, intelligence-based guidance from the Government would benefit universities' decision-making and engagement. Likewise, the University endorses a collaborative approach to monitoring and assurance reports that includes mutual information access and sharing of updates between universities and government.

Support from security agencies on practical issues could assist with some of the challenges faced by universities in determining risk. A higher level of advice from relevant agencies, as determined by those agencies as appropriate for dissemination, would underpin more adaptive and confident risk assessment by universities.

Provision of guidance for regulatory and compliance regimes

Regulators should provide clear and pragmatic guidance at the earliest opportunity on how to meet expectations of compliance, mitigating risk and reporting. The need for clarity and guidance is particularly relevant to requirements of the Higher Education Integrity Unit within TEQSA, which will focus on complex and evolving regulatory issues including cybersecurity, foreign interference and research integrity over time. It is similarly the case with understanding the definition, parameters and permutations of key terms like 'robustness' in *UFIT Guidelines*.

Regulatory direction and clarity in the form of guidance and enforcement notes will reduce uncertainty about the meaning and application of regulatory terms or phrases. This will reduce confusion and improve processes as compliance regimes are implemented across the sector. For example, the sector experienced opacity and confusion in the rollout of the *FITS Act* that impeded effective progress in building compliance regimes.

Guidance material content can at times be last minute and too generic or high-level to be helpful in implementing mechanisms to meet compliance requirements. The *Modern Slavery Act 2018* 'Guidance for Reporting Entities' material produced by the Department of Home Affairs is a good example of helpful and timely guidance material. DFAT has an opportunity to embrace best practice in the promulgation of *Australia's Foreign Relations (State and Territory Arrangements) Act*.

Intellectual Property

The University recommends that data should only be collected for specific and necessary purposes, with avoidance of information disclosure requirements that will inhibit or impede Australia's innovation and Research & Development. A scenario in which the Australian Government routinely requires details of commercial-in-confidence negotiations would put at risk the initiation or progression of those discussions to the detriment of global collaborations and Australian productivity. It will be important not to dissuade or set up barriers to productive early engagements that do not create legal relations. Further, the Government should give undertakings in any compliance regime to manage appropriately commercial-in-confidence material.

Recommendations:

- **Interventions should be consistent, coherent and complementary across the suite of government regulatory regimes. New regulations:**
 - Should be subject to a robust, independent regulatory impact statement to identify duplication and assess for whole-of-government complementarity.
 - Should adopt precise and targeted measures to provide certainty for universities and potential partners.
 - Manage sensitively commercial-in-confidence information under disclosure requirements to protect and encourage valuable global engagement and collaboration.
 - Be supported by an implementation Taskforce that provides from government and regulators clear and pragmatic guidance at the earliest opportunity on how to understand, apply and meet new legislated requirements of compliance, risk mitigation and reporting.
- **Collaboration, cooperation and continual improvement would be facilitated by:**
 - Clarification from Australian Government agencies on areas of responsibility, accountabilities and practical resources available to universities for security-related queries and scenarios.
 - Provision of real-time information exchange with key and trusted personnel.
 - Intelligence-based guidance from the Australian Government, including which tools should be used for assessments, to assist universities' decision-making about national security considerations in foreign engagement.
 - A mutual approach to updating and sharing monitoring and assurance reports.

D) Responses to foreign interference risk in other countries and relevance to Australian universities

The United States (US) scenario bears some similarities to the Australian experience to date. As in Australia, the past three years in the US has seen heightened awareness and increased activity on the issue of foreign interference within the research community. Since early 2018, 'federal funding agencies have issued new requirements and guidance, federal law enforcement agencies have increased prosecutorial activity, and Congress has signed new legislation and sought information on how the academic research community is responding to this evolving issue'.¹

¹ See: <https://www.ucop.edu/ethics-compliance-audit-services/compliance/research-compliance/foreign-influence.html>

In the US, the sectoral response was led from an early stage by national research funding bodies. In August 2018 the Director of the National Institutes of Health (NIH) sent the first of a number of 'Dear Colleagues' letters to universities and other research bodies to alert them to 'threats to the integrity of US biomedical research' and systematic programs of foreign influence. The NIH released reports in 2018 and 2019 identifying recommendations on communication and awareness; risk mitigation; and monitoring, actions, and consequences.

During 2019, the NIH letter was followed by 'Dear Colleagues'/similar letters from government policy leads, such as the Executive Office of the President (Office of Science and Technology Policy); the Director of the National Science Foundation; the Department of Defense; and others. Numerous determinations and prohibitions followed from different government fora including the US Senate, Congress and numerous departments.

Not long after the Australian *UFIT Guidelines* were released, on 19 November 2019, the United States Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations released its staff report titled *Threats to the US Research Enterprise: China's talent recruitment plans*.

Some distinctions to the Australian experience are observable:

- The scale of exposure in the US is much greater than in Australia, which has a vastly smaller R&D landscape, particularly in comparison to the university sectors.
- Anecdotally, the policy underpinnings in the US are more openly discussed with reference to specific countries. In contrast to Australia, the US has not consistently adopted a country-neutral approach.
- Australian universities are keeping pace with global counterparts in acting on security concerns. In contrast to the US, the Australian sector did not wait for policy changes by government funding bodies to act in relation to foreign interference risk. Policy changes by the Australian national research grant bodies (ARC and NHMRC) to address foreign interference risks, occurred quite recently in 2020.
- Anecdotally, the US university sector may have some structural elements that make it more vulnerable to undisclosed foreign influence and interference, such as (unpaid) lay-offs of research staff over summer, meaning significant activity can occur for an external party without good visibility for the primary research institute.
- Amongst other steps intended to mitigate the risk of undue foreign influence, some US government departments, including the National Science Foundation and Department of Energy, announced in 2019 that internal personnel and contractors cannot participate in foreign government talent programs.

In common with the Australian sector, US universities have responded rapidly to a changed operating context. Many of the challenges currently experienced by the Australian sector are in common with the US sector. The University of Melbourne's approach of continuous improvement is informed with reference to approaches taken by universities in the US.

The United Kingdom (UK) appears to be modelling its response on Australia's example. In November 2019, a Parliamentary Foreign Affairs Committee inquiry found evidence of foreign

interference on UK campuses and reported failings in protections of academic freedom. Relevant UK government departments were tasked to work together to mitigate the risks, while Universities UK, the umbrella organisation for 139 universities, was asked by the UK government to ‘address the full range of risks’ through a sector-led approach, supported by government.

In October 2020, the *Managing risks in Internationalisation: Security related issues* guidelines were released, providing detailed guidance for institutions on the considerations and measures they should take to guard against hostile interference and promote academic freedom. The UK’s guidelines are similarly oriented to Australia’s *UFIT Guidelines*, suggesting a commonality of experience and response, although notably in arrears of the early mobilisation in Australia that produced the *UFIT Guidelines*.

Looking at the UK and US – both significant global powers with powerful academic/R&D resources and substantial global footprints – it is evident that Australia, and its universities, are keeping pace with foreign risk related security recalibrations. Anecdotally, the Australian university sector and Australian Government’s partnership on the Taskforce is regarded as a strong practice model by overseas jurisdictions, having produced the *UFIT Guidelines* collaboratively and efficiently in 2019 and now well advanced in the process of implementation.

This analysis would place Australia’s efforts thus far as near the forefront of addressing these issues coherently, both as a government and a sector. The collaboration between the Australian Government and universities, and within the sector, speaks to this, as well as universities’ early movement on *UFIT Guidelines* implementation, in contrast to delayed or less coordinated approaches taken elsewhere.

Appendix A:

Snapshots of the University's global engagement

University of Melbourne's graduate researchers and international engagement

- Approximately one-third of Graduate Researchers have an international engagement during their candidature. This includes presenting their work at conferences, conducting fieldwork or meeting with international collaborators.
- In 2019, 639 individuals had 782 periods of Study Away outside Australia last year. Most (~77.5%) were for 3 months or less. 82 different countries were visited. The top three were: United States (16.6%), United Kingdom (11%) and Germany (8.2%).
- Overall 46.8% listed attending a conference as the primary reason for travel, however there is significant variation across Academic Divisions. 27 periods were for Graduate Researchers studying at a Joint PhD partner institution.
- In 2019, the University of Melbourne established several new International Research Training Groups (IRTGs) and associated programs to foster growth in numbers of jointly awarded PhDs with outstanding international universities. IRTG initiatives include:
 - Germany: energy-related research linking expertise and facilities at RWTH Aachen University.
 - France: partnership with French National Centre for Scientific Research (CNRS) and affiliated universities across the country.
 - United Kingdom: partnership with University of Manchester across all research areas of mutual interest and complementary capabilities.
 - Israel: partnership with Hebrew University of Jerusalem to expand and develop collaborative research in biomedicine.
 - India: Melbourne-India Postgraduate Academy partnership with three leading Indian Institutes of Technology as an ongoing platform for development of research collaboration with Indian partners.

University of Melbourne's arrangements with foreign entities

- As of September 2020, the University has 954 ongoing research engagements involving a foreign entity with 57 different countries. The University's main collaborators are the United States and the United Kingdom.
- 400-450 new research engagements are anticipated annually involving a foreign entity. If proposed research arrangements are counted, the number would increase by approximately 3-4 times, i.e. 1200-1600 proposed arrangements per year.
- Outside of research engagements, the University has a further 100+ active agreements which includes MOUs and partnership agreements, and a further 1000+ arrangements in the teaching and learning space, including foreign sponsored students, graduate and PhD programs and gifts/donations/bequests to the University.

Appendix B:

Examples of global research impact

Orygen, Youth Mental Health Australia

Orygen has recently received a \$33 million grant from the United States' National Institutes of Health (NIH) to develop models for predicting outcomes for young people who are at imminent and high risk of psychotic illness. To the best of our knowledge, this is the largest competitive grant that had ever been awarded by the NIH to Australian-led medical research. It involves collaboration with seven countries. The overall aim of this study is to better characterise and improve prediction of outcomes in the Clinical High Risk for psychosis clinical population.

This will lead to substantial benefits for clinical care, healthcare services, and for research in this field. The research will be completed through participants completing clinical interviews, neurocognitive tasks, brain scanning and imaging and provision of biospecimens. This information will help researchers and clinicians to make better predictions about outcomes, and to develop more personalised treatment plans for young people identified to be at a higher risk for developing psychosis.

Nossal Institute for Global Health

The Nossal Institute works on practical solutions to pressing global concerns. It combines real-world experience with scientific rigour, and supports global and regional partnerships and projects aiming to achieve resilient, sustainable and inclusive global health outcomes. For example, the Nossal Institute for Global Health's Collaboration on One Health Economic Research for Systems (COHERES) project is funded by the Australian Government to improve health security outcomes through collaboration between human and animal health sectors in Cambodia, Lao PDR and Vietnam. It also works with the Postgraduate Institute of Medicine (PGIM) of the University of Colombo in Sri Lanka, which is the only university in that country to provide specialist training of medical doctors. The Nossal Institute partners with PGIM to support and host PGIM trainees looking for exposure to international research experts on public health.

Australia China Joint Research Centre, Healthy Soils for Sustainable Food Production and Environmental Quality

The Healthy Soils for Sustainable Food Production and Environmental Quality Joint Research Centre (JRC) is one of six Centres co-funded by both the Australian and Chinese governments as part of the Australia-China Science and Research Fund (ACSRF), administered by the Commonwealth Department of Industry, Science, Energy and Resources. It is focused on delivering tangible economic, environmental and social benefits for both countries and specifically responds to an expressed industry need for improved soil sustainability and related food security tools. The University of Melbourne leads this Centre under the guidance of Professor Deli Chen who brings together expertise from across Australia including the CSIRO and the University of Western Australia, among others.

In China, the Centre is supported by ten partners including the Chinese Agricultural University, Chinese Academy of Sciences, and Nanjing Agricultural University. The Centre delivers new solutions to challenges in sustainable agricultural management and trains early and mid-career researchers in developing new technologies and management practices to improve farming productivity and sustainability for Australia and China. Since its inception, this team of experienced scientists and scholars have strictly adhered to both internal University policies and processes relating to intellectual property, conflict of interest and data security and management. Robust governance and risk mitigation strategies have been developed by the Centre, with all Centre activities complying with existing legislative frameworks relating to Australian and International export controls, DFAT visa screening and specific responsibilities and obligations specified in the Commonwealth Government funding agreement.

Addressing the global challenge to conserve irrigation water

This University of Melbourne-led research on efficient irrigation has led to widescale installation of irrigation systems in river basins around the world, improving water use efficiency and agricultural productivity in those areas by 30%. The technologies, developed in conjunction with industry, allow farmers to control irrigation automatically, rather than manually. This enables a significant decrease in the water delivery time, reducing risk to crops and loss of water. The hosting of overseas delegations at the University through the Australia-China Joint Research Centre, including delegations from China, Chile, and Mexico, was integral to the uptake and impact of the technology around the world.

Reducing the transmission of dengue in the tropics

The Queensland Department of Health, as well as the government health departments of Singapore, Kuala Lumpur, Malaysia, and Guangzhou (China), are changing the way they approach mosquito control and the spread of mosquito-borne diseases such as dengue, using a novel biocontrol method. This new approach is the result of extensive research undertaken by a team led by University of Melbourne researchers and longstanding collaborations with researchers at other institutions. This project's focus on controlling the transmission of mosquito-borne diseases benefits millions of people living in tropical regions where dengue is endemic, as well as local health services and health practitioners, businesses and tourism.

Preserving and recording the history and archaeology of the Gallipoli Battlefield for future generations

This globally-connected research contributed to a deeper understanding of the Gallipoli landscape and the experiences of soldiers who fought in the campaign. The Joint Historical-Archaeological Survey operated through the research was the first largescale, systematic study of the physical landscape of the Anzac Battlefield. It provided the governments of Australia, New Zealand and Turkey an opportunity to demonstrate to veterans' communities and also the general community, their united commitment to understanding and recording this point in history. The timing of the survey meant that many artefacts, which because of their age and exposure at Gallipoli were nearing the point of complete decay, could be recorded and preserved. Those that could be recovered and preserved are now housed at the Naval Museum at Canakkale.

Appendix C:

Cybersecurity at Melbourne

Cybersecurity Policy

The University maintains an Information Security Policy (MPF1270) and Provision and Acceptable Use of IT Policy (MPF1314) as part of the Melbourne Policy Framework to govern security for teaching and learning, corporate enterprise use, contracted service providers, contracted/funded research and collaborations, sensitive and classified information and international travel. These are reviewed on an ongoing basis to enable the University to respond to emerging threats or identified control deficiencies. The University aligns itself where possible to international standards such as ISO27001 and the NIST Cybersecurity Framework.

Cybersecurity Capabilities

The University deploys a range of technical controls and capabilities to help detecting and minimising the impact of cyberthreats against University systems:

- Next generation firewalls are deployed to inspect network traffic for anomalous or malicious traffic.
- Next generation endpoint protection technology is deployed across the University's fleet to protect against malware.
- Advanced email filtering services interrogate email for phishing emails and malicious attachments and links in email.
- Multi-factor authentication is enforced on all staff accounts across all key systems to reduce the impact of lost or stolen account credentials.
- Regular vulnerability scanning is undertaken across the University environment to detect weaknesses for remediation.
- Logging from key systems is aggregated centrally in a SIEM platform for analysis and detection of threats by our 24X7 Security Operation Centre.
- ITIL and specialised incident response processes are employed to quickly respond to problems and incidents.

Cybersecurity Governance

The University maintains an Information Security Council, which acts as the strategic steering group for all Cybersecurity matters and informs various University committees and councils in matters related to Cybersecurity. In addition, all changes to key University systems are overseen by several technology governance structures such as Change Review Board, Program Steering Group(s), and Architecture Review Board, in which the Cybersecurity team is included as a key stakeholder.

Cybersecurity culture and awareness

The University educates staff and students about cybersecurity fundamentals through a mix of online mandatory training, web-based awareness campaign material, printed collateral distributed around campus and events aligned with major University events such as O-week, Stay Smart Online Week and internal professional development sessions.

Strategic and continuous improvement

While the University has enhanced its overall Cybersecurity and resilience capabilities through the years, there is a continuous improvement program for Cyber Security including a current multi-year program to uplift cybersecurity capability further across the institution to help preparing for and responding to the constantly evolving cyber-risk threat landscape

Data Breach Reporting

The University has obligations regarding the collection, use and management of individuals' personal information under the *Privacy and Data Protection Act 2014* (Vic). To the extent that they apply to our activities, the University is also subject to the requirements of the *Privacy Act 1988* (Cth) and the European Union General Data Protection Regulation 2016/679. As part of its obligations, the University maintains a process that aligns with the key steps developed by OVIC for responding to a privacy breach and is activated when a privacy incident or suspected privacy breach occurs:

1. containing the breach and conducting preliminary assessments;
2. evaluating the risks associated with the breach;
3. taking steps to mitigate harm, including notifying relevant stakeholders and remediation;
4. reviewing the cause of the breach, the University's response, and taking steps to mitigate the risk of future breaches; and
5. reporting on the breach.

Appendix D:

The University's compliance requirements relating to foreign interference – a summary

Law/regulation/policy (Federal)	Administering government agency
<ul style="list-style-type: none"> Guidelines to Counter Foreign Interference in the University Sector 	Department of Education, Skills and Employment
<ul style="list-style-type: none"> <i>Australia's Foreign Relations (State and Territory Arrangements) Bill 2020</i> 	Department of Foreign Affairs and Trade
<ul style="list-style-type: none"> ARC Conflicts of Interest and Confidentiality Policy Australian Code for the Responsible Conduct of Research National Statement on Ethical Conduct in Human Research National Principles of Intellectual Property Management for Publicly Funded Research 	Australian Research Council National Health and Medical Research Council
<ul style="list-style-type: none"> <i>Foreign Influence Transparency Scheme Act 2018</i> <i>Foreign Influence Transparency Scheme Rules 2018</i> <i>Foreign Influence Transparency Scheme (Disclosure in Communications Activity) Rules 2018</i> 	Attorney-General's Department
<ul style="list-style-type: none"> <i>Higher Education Support Amendment (Freedom of Speech) Bill 2020</i> 	Department of Education, Skills and Employment
<ul style="list-style-type: none"> <i>Autonomous Sanctions Act 2011</i> <i>Autonomous Sanctions Regulations 2011</i> 	Department of Foreign Affairs and Trade
<ul style="list-style-type: none"> <i>Defence Trade Controls Act 2012</i> <i>Defence Trade Controls Regulation 2013</i> <i>Export Control Act 2020</i> <i>Customs Act 1901</i> 	Department of Defence
<ul style="list-style-type: none"> <i>National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018</i> 	Department of Defence ASIO Attorney-General's Department
<ul style="list-style-type: none"> <i>Security of Critical Infrastructure Act 2018</i> <i>Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020</i> 	Department of Home Affairs
<ul style="list-style-type: none"> <i>Criminal Code Act 1995</i> 	Attorney-General's Department

<ul style="list-style-type: none"> • <i>Privacy Act 1988</i> • <i>Australian Privacy Principles</i> 	Attorney-General's Department
<ul style="list-style-type: none"> • Inquiry into national security risks affecting the Australian higher education and research sector 	Parliamentary Joint Committee on Security and Intelligence
<ul style="list-style-type: none"> • Higher Education Integrity Unit 	Minister for Education Tertiary Education Quality and Standards Agency
Law/regulation/policy (State)	Administering government agency
<ul style="list-style-type: none"> • <i>The University of Melbourne Act 2009 (Vic)</i> • <i>The University Delegations Framework</i> 	Department of Education and Training (Vic)
University internal regulation	
<u>Policies that trigger Government action or engagement</u> <ul style="list-style-type: none"> • Research Integrity and Misconduct Policy • Research Ethics and Bio Management Policy 	
<u>Other policies and governance relevant to FI and compliance</u> <ul style="list-style-type: none"> • Risk Management Policy • Risk Roles and Responsibilities Policy • Advancement Policy • Gifts Policy • Staff Induction Procedure • Appropriate Workplace Behaviour Policy • Graduate Research Training Policy • Employee Travel Policy • Student Travel and Transport Policy • External Work Policy • Enterprise Risk Management Framework • Information Security Policy • Outside Work Procedure • Research Funding and Fee for Service Activities Policy • Research Ethics and Biorisk Management Policy • University Risk Register – Strategy Planning and Performance • Selection and Admissions Policy • Research Integrity and Misconduct Policy • Student Travel and Transport Policy 	