Response to the *Consultation Draft Guidelines to Counter Foreign Interference in the Australian University Sector*

6 September 2021

Executive Summary

The University of Melbourne welcomes the opportunity to respond to the *Consultation Draft Guidelines to Counter Foreign Interference in the Australian University Sector (*Draft Guidelines).

Australia's sovereign capability, protected by its national security apparatus, is strengthened by a highly proficient and competitive higher education and research sector. We recognise the continuing importance of protecting national security through raised awareness across the university sector and comprehensive management of foreign interference risks. Through the University Foreign Interference Taskforce (UFIT) collaboration, and in other ways beyond UFIT, the University is committed to strengthening its operating protocols, systems, and governance to mitigate identified foreign interference risks.

Since its establishment in August 2019, the UFIT model has been working effectively as a self-regulatory, co-designed set of Guidelines built through transparency and partnership. The refreshed Guidelines should maintain and embed those crucial attributes and establish the Guidelines as a permanent, collaborative cross-sectoral platform.

The refresh process is timely and will support the maturing of the sector's engagement and development of robust systems. It should aim to deliver refreshed Guidelines that are relevant to institutions' circumstances, support responsiveness to changes in the threat landscape, and deepen the two-way relationship between the sector and government agencies with shared accountabilities for the risk management of foreign interference.

Maintaining the partnership model of the UFIT Guidelines

The positive outcomes and international endorsements of the original UFIT model shows the efficacy of voluntary and co-designed guidance on best practice. However, in the Draft Guidelines there is a shift to a more prescriptive and compliance-orientated regulation. In view of this, throughout this submission the University recommends the Guidelines include a strengthened emphasis on self-regulation and partnership to build on the effective, educative, established model and continue to uplift practice across the sector. This would be assisted by formalising the UFIT Taskforce as a permanent cross-sectoral group with regular engagement with relevant Ministers, departments, and agencies.

There has been strong cross-agency endorsement of the success of the Guidelines and their underpinning approach. The Department of Home Affairs advised the Parliamentary Joint Committee on Intelligence and Security (PJCIS) that the adoption of the UFIT Guidelines had

achieved 'a heightened awareness by the sector of foreign interference risks and its capacity to mitigate the risks'.[1] The Department of Education, Skills and Employment submitted that 'the sector demonstrated its commitment to applying the Guidelines to bolster mitigation against foreign interference risks', including 'providing advice to Government in setting out their action and progress in implementing the Guidelines.'[2]

As well as balancing the need for action with the autonomy and diversity of institutions, the first phase of the UFIT model furthered a positive and open relationship based on mutual education and goodwill between government agencies and the sector in identifying and managing foreign interference risk.

The Director-General at the Australian Security Intelligence Organisation, Mr Mike Burgess, advised the PJCIS in a public hearing earlier this year that 'addressing national security risks doesn't need to come at the expense of academic freedom, which forms a core pillar of our universities and research institutions'.[3] In regard to the university sector's progress on the UFIT Guidelines to March 2021, he remarked:

> *I'm comfortable at this point in time with where the Guidelines are, but we know that that is a collaborative process and one that we should continue to focus on. It can't be 'set and forget', because the nature of the threat, how it comes at you and what they exploit changes all the time*.

The partnership model, in which the Commonwealth has ultimate responsibility for national security, should be retained in the refreshed UFIT Guidelines. In line with this, the Government's commitment to the collaborative process should be more pronounced in the Guidelines. The effective evolution of the Guidelines will require greater specificity on which risks, research, and technologies should be the focus of efforts to address foreign interference to ensure finite resources – in universities and government – are efficiently and appropriately targeted. While universities can undertake due diligence to an effective level, their ability to investigate and verify information is limited relative to government's purview.

Co-ordinate and build on existing systems

As well as shifting away from the partnership model, the Draft Guidelines do not appear to strengthen existing processes but instead introduce overlapping, mandatory and granular demands on institutions. As such the Draft Guidelines represent a move away from the prior approach (of integrating best practice into existing processes) to a new approach of requiring universities to set up parallel regulatory systems for foreign interference risk, siloed from other government-required activity in this regard. This development may inadvertently result in compliance activity that distracts institutions from the important risks that need managing. Proportionality should be built into the Guidelines, by identifying the areas of greatest risk of

[1] Written submission to the PJCIS from the Department of Home Affairs, 18 December 2020, p.12 (available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Submissions)

[2] Written submission to the PJCIS from the Department of Education, Skills and Employment, 18 December 2020, p.6 (available online - as above)

[3] *Official Committee Hansard: transcript of public hearing, 11 March 2021*, Joint Standing Committee on Intelligence and Security inquiry into the national security risks affecting the Australian higher education and research
Sector, p.26.

foreign interference and designing mitigations for those (as we do with Defence Trade Controls), rather than a blanket approach of detailed regulation.

More support for managing interference in campus life

The Guidelines also do not include sufficient guidance on managing foreign interference in campus life, which was identified as a concern and discussed extensively as part of the PJCIS hearings earlier this year. Universities would benefit from advice on managing foreign-backed political activity on campus, including protests and in the classroom and lectures, recognising that there are limits to university activity and influence outside of freedom of speech and academic freedom policies.

The power of government expert advice

The Guidelines are an opportunity to further strengthen the benefits of cross-sectoral partnership, including the flow of information from government to universities. Australian Government information, including departmental contacts (beyond central phone lines), practical tools and supports should be assured and made explicit in the Guidelines and Guidelines Guidance Material (GGM), including pathways for leveraging the expertise of relevant government agencies in relation to specific, higher risk issues and proposals. Universities are committed to uplifting foreign interference risk management, but reliable and accessible data is essential to the task.

<u>The UFIT Guidelines in the broader context</u>

Co-ordinating with other legislative and policy changes

The final report of the PCJIS, which scrutinised foreign interference risk management at universities, has not yet been released. In view of the wider policy and legislative context, the refreshed Guidelines should be linked and aligned to the full suite of legislative and policy changes – in train and ahead – that are relevant to protecting Australia's national interests. This would include recently established schemes on foreign arrangements and influence, anticipated changes through the *Security Legislation Amendment (Critical Infrastructure) Bill 2020,* and the forthcoming PJCIS inquiry report.

Intersection with previous UFIT Guidelines

There are also the previous UFIT Guidelines to consider. The consultation documents do not explain the relationship between the prior Guidelines and the refreshed Guidelines. This is a central consideration as universities are well advanced in reforms and implementation programs developed on the basis of, or heavily guided by, the first iteration of the Guidelines. Rather than siloed efforts in numerous areas of policy and regulation, reforms should be coordinated across government, coherent and mutually reinforcing.

Clarity for implementation timeline

Another practical issue that remains unclear is that of timelines for implementation. Given the extent of cyber and other due diligence changes that may arise from the refreshed Guidelines, implementation timelines for the refreshed UFIT Guidelines will need to be developed in close consultation with the sector.

Overview of this submission

In this response the University of Melbourne identifies ways to: (i) improve the Draft Guidelines and materials to enhance the effective partnership model and (ii) strengthen the university sector's capacity to responsibly manage foreign interference risks. This paper includes:

- Overview comments
- Key Recommendations
- Responses to specific sections of the Draft Guidelines and Guidelines Guidance Material (GGM).

In addition, we provide two appendices:

- Appendix 1: Textual revisions recommended by the University (in table form).
- Appendix 2: Summary of University of Melbourne activities and programs in alignment with the UFIT Guidelines.

For more information, please contact Professor Michael Wesley, Deputy Vice-Chancellor International on michael.wesley@unimelb.edu.au.

Recommendations

Self-regulation and progress reporting

1. The Guidelines and Guidance Material should reflect and express the collaborative, voluntary and adaptable foundations of the UFIT model, with a strengthened emphasis on self-regulation and partnership.
2. A light-touch reporting regime, proportionate to the risks being addressed and with explicitly stated scope and requirements, should be outlined in the refreshed Guidelines and Guidance Materials.

Role of government

3. The Guidelines should better reflect whole-of-government coordination as part of the UFIT model, including integration of recent, current, and upcoming changes in legislation and regulation relating to foreign arrangements and interference.
4. The Guidelines should encompass a role for intelligence-based, proactive guidance from the Australian Government to assist universities' efforts to build optimum risk frameworks, policies, and procedures for combating foreign interference.
5. Given its effectiveness to date, the UFIT Steering Group should be formalised as a permanent cross-sector taskforce on countering foreign interference at universities, engaging with relevant Ministers and officials across government and continuing its function as an educative, collaborative and information-sharing platform.
6. Australian Government information, including departmental contacts (beyond central phone lines), practical tools and supports should be assured and made more explicit in the Guidelines and Guidance Materials, including pathways for leveraging the expertise of relevant government agencies in relation to specific, higher risk proposals.

7. Implementation timelines for the next UFIT phase should be developed in close consultation with the sector.

Section 1: Governance and risk frameworks

8. Organisational risk should be explicitly referred to in the Guidelines as assessed and managed by institutional determination – informed by government advice and contemporary information on foreign interference – and security should be proportionate to organisational risk.
9. Risk frameworks and assessments in the Guidelines should be outlined at a higher level to allow full integration with universities' existing risk processes, and therefore capture monitoring and controls within mature oversight mechanisms.
10. The Guidelines should affirm proportionality by identifying the areas of greatest risk of foreign interference (akin to Defence Trade Controls) and enable Universities to design specific controls and mitigations for those risks.

Section 2: Communication, awareness, and education

11. The Guidelines should promote and enable an adaptive, context appropriate implementation approach from universities, and accordingly remove unnecessary prescriptiveness about delivery of training and communications programs to staff and students.
12. The Guidelines should emphasise the role and importance of university researchers in mitigating foreign interference risk and aim to build foreign interference risk literacy and responsiveness into national research codes, norms, and practices.

Section 3: Due diligence, risk assessments and management

13. The Guidelines should detail the role for government agencies to provide clear, timely and up-to-date guidance to the sector about which emerging technologies are considered sensitive or critical.
14. The University recommends Section 3 of the Guidelines provide higher-level objectives with clear mechanisms or pathways for universities to seek advice from government on proposed activities, partnership or research that have been assessed as high risk under the university's risk-based proportionality framework.
15. The Declaration of Interest disclosure form and sample questions provided at Appendix 1 are not fit-for-purpose. Instead, the Guidelines should utilise the original questions submitted by the Due Diligence Working Group, which are informed by sector-based experience and insight.

Section 4: Cybersecurity

16. To enable university cybersecurity teams to implement the Guidelines' objectives within their institutional contexts, the mandatory language in Sector 4 should be moderated or removed.

Section 5: Knowledge sharing

See also: Recommendations 3-7 above

17. The Guidelines should facilitate regular information and assessment exchange sessions between government agencies and specified university contacts.

General comment: compliance focus will undermine the objectives of the Guidelines

Considering the progress made under the first iteration of UFIT, universities can be expected to continue to demonstrate good faith management and best practice adoption of foreign interference risk mitigation.

Addressing foreign interference risk will be best achieved through government and universities working closely and collaboratively together. Too strong emphasis on compliance aspects may inadvertently undermine the objectives of the UFIT Guidelines – elaborate compliance requirements do not mean security will be protected and enhanced. University governance is multifaceted, robust, and systematic with numerous levels of accountability. The challenges are diverse across the sector. As the UFIT model has successfully shown, universities are best placed to work out how to implement the UFIT objectives within their contexts.

To do so, universities need clear-eyed assessments and two-way communication with light touch reporting to keep them on track and to facilitate shifts when the risks evolve and change. The Guidelines should be imbued with this approach, with regular check-ins with the sector to gauge progress.

In its current form, the mandatory language used in the Draft Guidelines sections/clauses read as strict requirements, rather than guidelines: e.g., 'the guidelines provide baseline actions *to be adopted* sector-wide". This approach will undermine the good work that has occurred under the previous iteration of the Guidelines, which developed a mutually reinforcing and trusting relationship between government agencies and universities that implicitly recognised the alignment of interests that both sectors have in addressing foreign interference risks.

The mandatory language also raises the prospect of formalised regulation and higher compliance requirements around the UFIT Guidelines. While light-touch reporting (as already occurs) is to be expected, a significantly more onerous reporting and compliance burden is inappropriate for the UFIT model and saps institutional resources from the work of managing real risks. Foreign engagements are already subject to close and increasing regulation through existing legislation, including the Foreign Arrangements Scheme, the Foreign Influence Transparency Scheme, Defence Export Controls, and research funding channels including the Australian Research Council. Given the imminent report of the PCJIS, the University recommends transparency and collaboration should continue in the approach to UFIT implementation and compliance.

The University affirms the points made on page 5 of the Draft Guidelines, that the first Guidelines were a world-leading innovation that supported 'the development of sophisticated risk management frameworks and practices', while upholding the 'foundational principle of university accountability and autonomy'. A benefit of the previous UFIT Guidelines was their capacity to support sector-wide uplifting of capability and preparedness, while enabling implementation methods as appropriate to each university's context. The previous Guidelines were also crafted to enable institutions to respond to evolutions in foreign interference risk over time.

This flexibility and adaptability were recognised by representatives of the Australian Government, including former National Counter Foreign Interference Coordinator Mr Chris Teal, who advised the PJCIS that:

> *institutions have a different profile in relation to the foreign interference threat that they face, and that profile is based upon the nature of the research, the location and the like. Therefore, in thinking about the [first UFIT] Guidelines we have done to date,* ***flexibility, scalability and adaptability*** *are particularly important as we are thinking about the future [our emphasis].*

It is this spirit that should be retained and embedded in the refreshed Guidelines.

Guidelines Guidance Material (GGM)

Overall, the GGM is a useful and appropriate source of reference points and questions. However, the language used in the GGM document is at odds with the Draft Guidelines, as the latter includes numerous prescriptive points that read as mandatory requirements.

Conflicting approaches between the Guidelines and the GGM's respective use of voluntary/mandatory language will cause uncertainty and waste compliance resources for both universities and government agencies as we seek to resolve conflicting interpretations when implementing the refreshed Guidelines.

Recommendation 1: The Guidelines and Guidance Material should reflect and express the collaborative, voluntary and adaptable foundations of the UFIT model, with a strengthened emphasis on self-regulation and partnership.

General comment: compliance and reporting

Streamlining the reporting and compliance burden in explicit terms in the Guidelines and GGM would avoid undue burden or duplication. The previous Guidelines necessitated operational and governance changes within universities, as will the refreshed Guidelines – this is the point of the undertaking.

The Draft Guidelines on page 6 state that 'these Guidelines are not intended to place additional regulatory burdens on universities'. While a welcome intention, it is inevitable and appropriate that the refreshed Guidelines will require a continuation of practical communication, feedback, and periodic reporting by universities to government. It is important, however, that this reporting is identified and kept to a reasonable level. If, for example, it is envisaged that there will be a requirement for an annual report from universities on implementation and compliance, this should be clearly articulated and its scope and rationale made explicit.

The University is committed to comprehensively countering foreign interference and associated risks across its domain. Nevertheless, the numerous reforms to law and regulation over recent years have added significant regulatory burdens and costs to universities. In some instances, such as the Foreign Arrangements Scheme, new regulations have generated substantial confusion and workload within the university sector and government about crucial implementation details, hampering synergy and effectiveness of universities' governance structures and resource planning.

Given the challenge presented by proliferating and uncoordinated regulation, any new reporting or compliance burden should be feasible, specific, integrated, and able to be

measured. Coalescing the numerous siloed government reforms and compliance obligations should also be a priority.

Recommendation 2: A light-touch reporting regime, proportionate to the risks being addressed and with explicitly stated scope and requirements, should be outlined in the refreshed Guidelines and Guidance Materials.

General comment: the role of government and security agencies

Proactive engagement, information, and collaboration with Australian Government agencies

UFIT is a forum with a clear agenda for the sector to come together to consult on issues with government agencies. UFIT remains a unique opportunity for Australian Government agencies to play a more active role in guiding universities through information sharing to inform a more targeted approach to protecting national interest.

On Page 6, the Draft Guidelines state that 'security is a collective responsibility with individual accountability'. As it stands, the Draft Guidelines do not share the burden of this collective responsibility proportionately. Former Deputy-Secretary of the Department of Education, Skills and Employment, Mr Rob Heferen, advised the PJCIS in March 2021, 'one of the key things in the guidelines, and the approach government has taken, is a need for a proportionate approach, so that's quite important'.[4]

Much emphasis is placed in the Draft Guidelines on university-driven actions to develop appropriate policies and processes. The University recognises that this is the primary point of the UFIT model – to collaborate, co-design and build good risk management, disclosure processes, accountable authority, escalation and reporting process, communications and education, due diligence, and cyber security practices across the sector.

Implementation of the Guidelines will be better targeted and executed over time if they are informed by continual and detailed guidance and feedback from expert Australian Government agencies. Communication channels need to be formalised and coordinated at the government end to ensure maximum effectiveness of the Guidelines.

The Australian Government has the wider perspective and access to information about national interest risk that can guide universities' good practice. Through UFIT and the refreshed Guidelines, a joined-up and collaborative partnership approach between universities and government should be further embedded, including improved communications and information flows. This could be facilitated by adoption of a whole-of-government approach on managing risks and regulatory reforms relating to universities.

The recently implemented Foreign Arrangements Scheme, in which the burden of risk and response assessment lies with universities, gives rise to situations in which universities are asked to interpret and make decisions on national foreign policy and security that are outside of their expertise or line of sight.

Similarly, in the Draft Guidelines, the role of government is insufficiently articulated and benchmarked. The Draft Guidelines would benefit from a much clearer articulation and

[4] *Official Committee Hansard: transcript of public hearing, 11 March 2021*, Joint Committee on Intelligence and Security inquiry into the national security risks affecting the Australian higher education and research sector, p 20.

practical examples of how Australian Government departments should work together to contribute information, expertise, and feedback through UFIT to the University sector.

Ambiguous commitment to action in the Draft Guidelines is illustrated by language suggesting that government agencies '*may* be able to help' with certain activities (e.g. page 18). In order to strengthen their effectiveness, the refreshed UFIT Guidelines should have expressions of baseline commitment to proactive engagement and provision of information – for universities and government.

Recommendation 3: The Guidelines should better reflect whole-of-government coordination as part of the UFIT model, including integration of recent, current, and upcoming changes in legislation and regulation relating to foreign arrangements and interference.

Recommendation 4: The Guidelines should encompass a role for intelligence-based, proactive guidance from the Australian Government to assist universities' efforts to build optimum risk frameworks, policies, and procedures for combating foreign interference.

Make UFIT a permanent cross-sectoral taskforce

The refresh consultation has not shed light or detail on the future of the overall UFIT process. As it stands, the collaborative process is voluntary, relatively informal, and primarily focused on the production of key outputs, including collaborative discussions across the sector. To date there has also been a heavy focus on setting up, and updating, the Guidelines. UFIT has worked effectively with these characteristics and settings.

However, there would be value in adapting the UFIT Taskforce and Steering Group into a permanent cross-sectoral taskforce on combating foreign interference in universities, charged with information sharing, mutual education, and best practice delivery. This would enhance the connections and engagement between stakeholders, relevant Federal Ministers and departments/agencies, while providing a continued channel for developing governance, and balancing industry issues with national interest considerations.

Recommendation 5: Given its effectiveness to date, the UFIT Taskforce should be formalised as a permanent cross-sector taskforce on countering foreign interference at universities, engaging with relevant Ministers and officials across government and continuing its function as an educative, collaborative and information-sharing platform.

Whole-of-government coordination – agencies and contacts

The GGM attachments include a section on Government Contacts, which provides clarification at a very high level on Australian Government agencies' areas of responsibility. The number of key agencies listed in this section demonstrates how widely the issue of foreign interference reaches across government, including in relation to the university sector's preparedness and management.

It would be appropriate for government to be clearer about which department will act as the primary point of contact for the sector for matters related to foreign interference, to provide direct communication channels for the sector, and to actively assist the sector as universities continue implementing the Guidelines. The leading option would be for the Counter Foreign Interference Coordinator within the Department of Home Affairs to assume this role.

As part of clarifying roles, clearly defined pathways for engagement with appropriate government agencies for specific activities assessed by a university as high risk should also be articulated through UFIT or otherwise.

As part of this governance, the Guidelines should also articulate which area of government will be the primary interface for universities' reporting on foreign interference progress through the new UFIT Guidelines. Again, this should be an area with knowledge expertise such as the Department of Home Affairs.

There should be further sector consultation on light touch reporting arrangements that show how UFIT has guided university work to address foreign interference and an implementation timeframe should be outlined.

Recommendation 6: Australian Government information, including departmental contacts (beyond central phone lines), practical tools and supports should be assured and made more explicit in the Guidelines and Guidance Materials, including pathways for leveraging the expertise of relevant government agencies in relation to specific, higher risk proposals.

Recommendation 7: Implementation timelines for the next UFIT phase should be developed in close consultation with the sector.

Section 1: Governance and risk frameworks

Setting risk frameworks and managing risk (1.1, 1.4-1.5)

On page six of the Draft Guidelines, the principle is given that 'security should be *proportionate to organisational risk*'. The University assumes organisational risk to be a matter of institutional determination and this should be explicitly clarified and consistently reflected in the Guidelines. The Draft Guidelines should confirm the autonomy of each institution to assess and protect against risk.

As part of this, universities must set their own risk appetite, informed by external requirements and other information on foreign interference risks and technologies. The University of Melbourne has a well-developed approach to risk frameworks, risk registers and key risk indicators, with an expectation of continuous improvement and regular review. By setting out features of risk frameworks and features to a highly specific level, the Draft Guidelines impose a particular and granular risk assessment on certain areas of university activities, which essentially requires parallel, rather than integrated, risk framework processes. To avoid this while retaining the core purpose of the risk frameworks, the elaborative points under Draft Guidelines 1.1-1.5 should approach governance and risk frameworks at a higher level.

The University endorses the statement at 1.1 that 'government provides advice on foreign interference threats to help universities identify and manage risks'. As addressed in other parts of this submission, greater provision of latest information will enhance universities' decision-making and management of foreign interference risk.

Recommendation 8: Organisational risk should be explicitly referred to in the Guidelines as assessed and managed by institutional determination – informed by government advice and contemporary information on foreign interference – and security should be proportionate to organisational risk.

Recommendation 9: Risk frameworks and assessments in the Guidelines should be outlined at a higher level to allow full integration with universities' existing risk processes, and therefore capture monitoring and controls within mature oversight mechanisms.

Recommendation 10: The Guidelines should affirm proportionality by identifying the areas of greatest risk of foreign interference (akin to Defence Trade Controls) and enable Universities to design specific controls and mitigations for those risks.

Policies and training on responsibilities and conduct (1.3)

Draft Guidelines 1.3-1.4 refer to the communication and provision of information and training about foreign interference frameworks and policies to all 'staff and students'. The Glossary clarifies that '*staff and students*' throughout the Draft Guidelines refers to academic staff, professional staff, undergraduate students, postgraduate students, PhD (and doctoral) students, visiting staff or honorary appointments. Notably, this definition captures wide and distinct cohorts within the university community.

The specificity about training and support across 'staff and students' should be removed from the elaborating points under 'Universities should consider'. Training will only be effective if it is meaningful to the relevant cohort (staff, students, for example) and is attuned to the risk profile of different disciplinary areas. Training is to present any foreign interference issues through the mechanisms of export controls or sensitive/critical technologies, or with reference to foreign influence in research or teaching.

The Guidelines should enable universities to determine how to maximise the take-up of training, potentially through encouraging and facilitating the sector to share approaches and develop best-practice training and communication. Based on experience, a universal mandatory approach of one-size-fits-all training is ineffective in securing the outcomes required and does not in itself guarantee broad-based understanding of foreign interference risk and management. Given this issue also appears at 2.1, training and awareness requirements should be streamlined throughout the Draft Guidelines.

Section 2: Communication, awareness, and education

The University strongly affirms the overall objective in Section 2 that universities should build a supportive and resilient culture in university communities. Resilience against foreign interference is recognised by our institution as a continuing priority. At the University of Melbourne, integration of these risks into existing reporting and governance structures enables oversight at the most senior levels of the institution. A range of educative and communication initiatives further develops a culture of awareness and uplifts risk literacy.

As outlined in Appendix 2, the University has also established 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. The refreshed UFIT Guidelines will be an important factor supporting universities to continue progress on building a culture of risk awareness and responsibility.

Training to staff and students (2.1)

The University makes informed and prudent decisions about the provision and/or availability of training to staff and students. For instance, it already provides:

- an advanced set of outreach and training programs to academics and professional staff (e.g. on the Foreign Influence Transparency Scheme);
- upskilling courses to legal and compliance staff about various regulatory developments; online training modules and resources on foreign interference that are available to all staff and mandatory for many in research and philanthropy;
- in-person/virtual Know Your Partner training for relevant research and academic staff; and
- in-person/virtual information sessions on risk and responsible research as part of induction for new staff, new graduate students and as part of research supervisor training.

Further information about training and other workstreams relevant to the first UFIT Guidelines is attached at Appendix 2.

Recommendation 11: The Guidelines should promote and enable an adaptive, context appropriate implementation approach from universities, and accordingly remove unnecessary prescriptiveness about delivery of training and communications programs to staff and students.

Alignment and integration with research codes and ethics (2.1-2.2)

In the current documents, researchers are not a key focus of the Draft Guidelines, including in section 2. However, managing foreign interference heavily relies on researchers' awareness and capacity to identify and respond to the risks. The success of the UFIT objectives will be substantially influenced by the degree to which the UFIT enhancements and learnings penetrate Australia's research community, as they are typically both the first line of defence for identifying foreign interference issues and potentially problematic research applications. For instance, when assessing the potential dual-uses of research and technology, researchers are a university's best resource due to their expertise. They are also the government's best resource where our research is at the cutting edge of a field, such as quantum computing.

The University has been rolling-out comprehensive programs of risk literacy and foreign interference training to raise awareness amongst our academics that managing foreign interference at all career stages is vital to protect their research, reputation, and intellectual property, and that this aligns with university and national interests.

Given the central role of researchers, the University sees great value in integrating foreign interference management practices with researchers' overall commitment to responsible research practices. Rather than being permanently exceptionalised, this area should, as far as possible, become fully aligned and integrated with national research codes and practices and due process at universities. Where programs that deal with specific forms of legislation are required (such as training about the introduction of the FITS), these could be overlaid, which already occurs at the University of Melbourne.

The Guidelines should include a clearer emphasis on the role of researchers in being risk aware and responsive to foreign interference, and the alignment of research interests and national interests. In this vein, it would be appropriate for the documents to highlight the personal and professional benefits to individual researchers of meeting research obligations and national security expectations, while protecting their work, research objectives, reputation, recognition, and Intellectual Property (IP).

Recommendation 12: The Guidelines should emphasise the role and importance of university researchers in mitigating foreign interference risk and aim to build foreign interference risk literacy and responsiveness into national research codes, norms, and practices.

Section 3: Due diligence, risk assessments and management

Most of the due diligence requirements (partner and research) in the Draft Guidelines roughly map across existing Export Controls processes, and as such can be integrated within current practices. However, some aspects of Section 3 should be described with more clarity and specificity relating to the government's role.

Government expertise to inform assessments (3.2.2)

At page 13, critical and emerging technologies are flagged in the Section 3 opening principles as being at highest risk of foreign interference. Effective management of this by universities will rely on Australian Government agencies identifying these risks to the sector with specificity, on the understanding that these are over and above the technologies identified on the Defence Strategic Goods List.

Section 3.2.2 says Government agencies '*may* be able to provide support' to universities for complex technology assessments (our emphasis). The Draft Guidelines at 3.2.2 should include a clear and unequivocal role for government agencies to provide specific, timely and up-to-date guidance about which technologies are considered critical or sensitive.

Recommendation 13: The Guidelines should detail the role for government agencies to provide clear, timely and up-to-date guidance to the sector about which emerging technologies are considered sensitive or critical.

Foreign arrangements and affiliations (3.2)

Section 3.2 has wide parameters as currently framed. As raised above in the discussion on critical technologies risk assessments, universities' performance of due diligence related to 3.2 would be greatly enhanced by provision of a pathway to seek advice on specific cases that are assessed as high risk under University-defined parameters. The Guidelines should establish and outline a process by which:

- Universities conduct risk assessments, informed by due diligence proportionate to institutional risk appetite and compliance requirements.
- Where that assessment process identifies high risk activity that the university wants to proceed with, universities need a pathway to test our decision-making with government, which may have access to information and insights that the university does not.

One of the problems encountered in the implementation of the Foreign Arrangements Scheme is that it is country agnostic, which wastes time and resources. From the University's perspective and experience, building capability and accuracy in the risk assessment component is the most important and meaningful aspect, rather than losing time looking at low-risk activities, institutions, or jurisdictions.

Risk-based framework to ensure due diligence remains relevant and comprehensive (3.1-3.4)

In recognition that universities do not have the same access to information as government, Section 3 of the Guidelines should provide pathways to government for universities to seek specific advice for proposed activities that are assessed as high risk under its own risk frameworks. For greater clarity on this, this section of the Guidelines would benefit from the insertion of a risk-based/proportionality framework as part of best practice due diligence (as utilised in Section 4 on Cybersecurity) rather than the granularity expressed in the current wording. Universities can work with more general and high-level objectives, and can supplement this by seeking advice where necessary.

Recommendation 14: The University recommends Section 3 of the Guidelines provide high-level objectives with clear mechanisms or pathways for universities to seek advice from government on proposed activities that have been assessed as high risk under the university's risk-based proportionality framework.

Declarations of Interest disclosures (3.1)

Appendix 1, which provides questions relevant to the Draft Guidelines on declarations of interest (DoI) disclosures, is not workable in its current form and should be redrafted.

Prescribed questions as currently outlined by Appendix 1 create a tension at the university end between compliance with the Guidelines, and compliance with the questions. Universities need implementation flexibility to bring UFIT processes into existing systems and the ability to responsibly adapt due diligence to the evolving landscape of risk.

The sample DoI questions attached to the refreshed Guidelines may be useful to some universities, but in the current form they appear to be compulsory for all. Any sample DoI questions and guidance points to be provided in Appendix 1 should only be indicative/suggestive and this should be explicitly stated. The University recommends the Guidelines utilise the sample questions submitted by the working group.

Recommendation 15: The Declaration of Interest disclosure form and sample questions provided at Appendix 1 are not fit-for-purpose. Instead, the Guidelines should utilise the original questions submitted by the Due Diligence Working Group, which are informed by sector-based experience and insight.

Section 4: Cybersecurity

In many cases the Draft Guidelines on cybersecurity may represent a scaling-up of, and/or potentially new forms of cyber due diligence as cybersecurity checks and assurances are woven throughout the Guidelines. As it will have an operational impact on the cybersecurity (and other) workloads at universities, this scaling-up of cyber due diligence should be considered in the setting of UFIT implementation timelines.

As with other parts of the Draft Guidelines, the language in the Draft Guidelines Section 4 on cybersecurity emphasises mandatory actions, strategies, and functions. Noting that throughout the first phase of the UFIT Guidelines universities, including Melbourne, substantially invested in their cybersecurity capability to expand expertise and risk management, the University recommends that the existing mandatory language in the Draft Guidelines be altered to enable universities' cyber teams to decide how to best implement cyber strategies to meet the UFIT Guidelines' aims and objectives. Cyber security teams will not be assisted by overly specific or mandated requirements that require interpretation or do not fit the university context.

Recommendation 16: To enable university cybersecurity teams to implement the Guidelines' objectives within their institutional contexts, the mandatory language in Sector 4 should be moderated or removed.

Section 5: Knowledge sharing

The Commonwealth has ultimate responsibility for national security and this needs to be reflected in the UFIT Guidelines. Potential government contributions are flagged at several points in the Draft Guidelines, however the government's commitment and expert input to the process should be more pronounced. For example, while a university may ask for full disclosure of conflict of interests, affiliations and funding sources, there are limits to the ability of universities to verify these. Universities will rely on the additional resources and experiences of government agencies such as ASIO to assist.

Recommendation 17: The Guidelines should facilitate regular information and assessment exchange sessions between government agencies and specified university contacts.

As discussed above, knowledge sharing could be also enhanced in the following ways:

- The Guidelines should reflect whole-of-government coordination as part of the UFIT model, including integration of recent, current, and upcoming changes in legislation and regulation relating to foreign arrangements and interference.
- The Guidelines should include detail on the roles and responsibilities of government departments and security agencies, with communication channels formalised and coordinated at the government end to ensure maximum effectiveness of the Guidelines.
- Stronger emphasis in the Guidelines on security agencies providing information to the sector for due diligence and cyber due diligence, such as identifying risks, or red-flagging potential partners or regions.

See also:

Recommendation 3: The Guidelines should better reflect whole-of-government coordination as part of the UFIT model, including integration of recent, current, and upcoming changes in legislation and regulation relating to foreign arrangements and interference.

Recommendation 4: The Guidelines should encompass a role for intelligence-based, proactive guidance from the Australian Government to assist universities' efforts to build optimum risk frameworks, policies, and procedures of combating foreign interference.

Recommendation 5: Given its effectiveness to date, the UFIT Taskforce should be formalised as a permanent cross-sector taskforce on countering foreign interference at universities, engaging with relevant Ministers and officials across government and continuing its function as an educative, collaborative and information-sharing platform.

Recommendation 6: Australian Government information, including departmental contacts (beyond central phone lines), practical tools and supports should be assured and made more explicit in the Guidelines and Guidance Materials, including pathways for leveraging the expertise of relevant government agencies in relation to specific, higher risk proposals.

Recommendation 7: Implementation timelines for the next UFIT phase should be developed in close consultation with the sector.

APPENDIX 1

Recommended textual revisions

Guidelines: 1.2, 2.2, 3.3, 4.2, 5.1, Guidelines: 3.4	"universities will…" "universities have…" (4.2) "*Universities will* implement a cyber security strategy that treats cyber security as a whole-of-organisation human issue and incorporates an appropriate controls framework".	*Replace with:* Language that is less prescriptive, such as universities should: "encourage"; "assess and take reasonable steps"; "as appropriate,…"; "consider establishing". Replace with guidance terminology such as 'cybersecurity should be seen as a whole of organisation…"
Page 6 (in the boxed text)	"Government supports to UFIT implementation e.g. providing updates to the sector on the prioritisation of key critical technologies of national interest to Australia"	Updates of this kind would greatly assist universities' management of Export Controls and foreign interference assessments. *Amend:* This Guidelines should include more explicit articulation of who/when/how this information will be made available to universities.
Page 7 'Reporting Requirements'	"Universities can use the data and reporting generated from the adoption of these Guidelines to promote their approach to counter foreign interference across the sector and to Government in line with university governance processes, for example in university Annual Reports. The Government may also seek assurance from universities that their approach to counter foreign interference align with these Guidelines and is proportionate to their risks".	*Amend:* As discussed in the submission, the compliance/reporting requirement associated with the refreshed Guidelines should be more clearly stated. It should be reasonable, proportionate and effective. Regarding reporting, we also highlight the annual reporting requirements to the State Government in universities' enabling legislation.

Page 8	3.2 Universities conduct due diligence to inform decision-makers of foreign interference risks.	*Amend* 3.2 Universities conduct risk assessment to inform decision-makers of foreign interference risks.
Page 11	Bullet points under 'universities should consider'	*Remove* 'how they train and support all staff and students' *Replace with*: 'universities should provide appropriate education, training and supports'
Page 12	2.1: "Staff and students receive training on, and have access to information about how foreign interference can manifest on campus and how to raise concerns in the university or with appropriate authorities."	*Replace with*: 'Staff and students, particularly those working in higher risk or risk exposed areas, *have access to appropriate training and information'…*
Page 12	2.1 (bullet 3) Universities communicate their expectations of appropriate conduct, and consequences if not met, to those using the campuses for their own activities, including student associations and hosts of public events.	This point is too prescriptive. Universities can achieve the headline point under this section without the prescriptive outline of what universities must tell student associations and public event hosts. The University of Melbourne already has relevant policies including: Student Conduct Policy; the Student Clubs – University of Melbourne Student Union Policy; the Freedom of Speech Policy; the Property Policy; the Appropriate Workplace Behaviour Policy; and the Academic Freedom of Expression Policy. The University of Melbourne Student Union (UMSU) expressly prohibits all forms of unacceptable behaviour. Unacceptable behaviour includes: bullying; discrimination; harassment (including sexual harassment); victimisation; vilification; or permitting, assisting or encouraging others to bully, discriminate, harass, victimise or vilify; or failing to treat others with dignity, courtesy and/or respect.

Page 12	2.2: Universities will provide training to staff and students who are engaged in foreign collaboration or other partnership activities at risk of foreign interference.	This duplicates point one, which encompasses collaboration and partnership as risk activity areas for universities.
Page 13	Paragraph 1 "Due diligence helps to identify and assess the level of risk of foreign interference. Transparency is key. Due diligence is conducted before activities at risk of foreign interference commence and is regularly reviewed in accordance with university policies and procedures. Universities seek to develop a culture of continuous disclosure."	*Amend to:* Risk assessment of activities at risk of foreign interference occurs in accordance with university risk frameworks, policies and procedures, both prior to commencement, to inform decision-making, and as appropriate during the activity. Due diligence helps to identify and assess the level of risk of foreign interference through creating transparency of relationships and influences. Universities seek to develop a culture of continuous disclosure.
Page 13	Paragraph 2 "Working with actors whose legal systems, approaches to academic freedom and human rights that do not align with our own, carries a higher risk of exposure to undue influence or acts that can undermine not only a university's security but also Australia's national interests".	This statement indicates a category of higher risk actors relevant to this policy reform – i.e. those with higher risk legal systems, academic systems and human rights records. These risk indicators should be used to better target compliance activity under UFIT and the Guidelines.
Page 13	3.2: Universities conduct due diligence to inform decision-makers of foreign interference risks. Due diligence is conducted on research activities, partners, and university staff and research students at risk of foreign interference.	Rather than conduct due diligence on all staff and research students, a risk-based approach should focus on activities as a trigger for risk assessment. *Amend to:* Due diligence and risk assessment is conducted on activities, partners, and university staff and students engaging in activities that present a risk of foreign interference.
Appendix 1 Page 19 Core Declaration of	Are you receiving any financial support (cash or in-kind) for research related activities from a country outside Australia?	*Delete as is not fit-for-purpose.* Replace with the original questions drafted and submitted by the working group.

Interest Questions and Guidance	Outline the obligations that you have to any foreign institutions (including other academic bodies, research entities or private industry) or governments. This includes paid and unpaid roles and/or honorific titles with academic bodies, research entities, private industry or governments.	*Delete as is not fit-for-purpose.* Replace with the original questions drafted and submitted by the working group.
	Outline any associations with foreign political, military, policing and/or security organisations.	*Delete as is not fit-for-purpose.* *Replace with the original questions drafted and submitted by the working group.* Question 3 is ambiguous around "association". This is a wide usage – for example, in its current form it could cover an Australian academic agreeing to be on a panel sponsored by a national war college in another country or events sponsored by foreign political, military, political or security organisations.
	Information should cover the past 10 years.	*Amend:* 'Information should cover the previous 5 years', as this is more likely to achieve the accurate disclosures sought and is a duration of time that is sufficient for due diligence.
Page 16	3.2: "Cyber security strategies set out"… and eight bullet points below this.	As per previous revision box, this should be altered to "Strategies include but are not limited to…" to enable individual university autonomy on how to meet the Guidelines.
Page 18	5.2: "Government will support the sector through raising awareness, sharing information relating to foreign interference and being accessible. Government agencies may be able to help universities identify" instances, or attempts, of foreign interference.	*Amend:* Expand and enunciate critical roles for government. For instance, more specificity regarding which agencies or Minister, and how information will be made available to universities.

Page 20 Glossary	"Espionage is the theft of Australian information by someone either acting on behalf of a foreign power, or intending to provide information to a foreign power which is seeking advantage".	*Amend:* Espionage can also occur in a domestic (Australian) setting, and is not specific to foreign interference.
GGM page 2	'University *policies* should consider the following key elements'	*Amend:* Insert 'and procedures' after 'policies' to be consistent with the main Guidelines.
GGM page 6	'Universities can provide training to staff, students and honorary appointments on..'	*Amend:* 2.2 in the Guidelines says universities *will provide* training. The Guidelines should be amended to reflect the GGM language to ensure consistency across the documents.
GGM page 7	Foreign Interference Transparency Scheme (FITS) [hyperlink]	*Correction:* This should be 'Influence', not interference
GGM page 15	Second last dot point "How do staff understand what risks should be shared with government agencies?"	Amend: The Government should provide guidance on what level of detail and category of information updates should be provided to government agencies by universities.

APPENDIX 2

University of Melbourne activities and programs in alignment with the UFIT Guidelines

August 2021

Governance and risk frameworks

- Oversight of the implementation of the University Foreign Interference Transparency (UFIT) Guidelines has been led by the University Foreign Interference Working Group (UFI WG), a sub-committee of the University's existing Research Due Diligence Advisory Group.

  Members of this Working Group are senior University representatives from Legal and Risk, Research Innovation and Commercialisation, Information Technology, Human Resources, Chancellery International, Advancement, Chancellery Research and Enterprise and Academic Divisions.

- The Working Group has oversight of the implementation of the UFIT Guidelines and the University of Melbourne is well advanced in progressing a staged UFIT Action and Implementation Plan.

- A number of other working groups and committees drawing on senior leadership across University areas have been established to ensure oversight and risk management is comprehensive and responsive (e.g. the Geopolitical Risk Advisory Group).

- In 2019, an environmental scan and gap analysis led by the Deputy Vice-Chancellor, Research identified many existing mechanisms, processes, and protections already in place within the University, as well as areas that needed strengthening.

- Upskilling University lawyers to review all material contracts in order that they can identify any potential risk for foreign influence and then raise with relevant contract owners to assist with an assessment of foreign influence risks in accordance with the *Foreign Influence Transparency Scheme Act 2018* (Cth) and the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*.

- There are currently two project teams (one staff, one student related) working through a series of recommended actions to uplift the University's international travel policy, procedure, process, practice and supports.

- Between Jan-July 2021, the University undertook a rigorous program of activity to meet its compliance obligations under *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*. Thousands of current arrangements, across the University and its controlled entities have been assessed, and approximately 650 registered.

Communication, awareness, and education

- In 2020-21, the Research, Innovation and Commercialisation Group has offered 'Know Your Partner' due diligence training and the Office of Research Ethics and Integrity will continue engagement with the Australian Sanctions Office to offer annual DFAT-conducted sanctions training. The Legal and Risk Unit have also developed general compliance training modules that are now available for all staff relating to the Foreign Influence Transparency Scheme Act 2018 (Cth) and Australia's Foreign Relations (State and Territory Arrangements) Act 2020.
- A suite of education and training programs are in place to educate and increase awareness among staff and students of risks, including: Research Integrity Online Training (RIOT); and online modules such as 'Conflict of Interest – Research', 'Key Policies and Information for Academics' and the mandatory 'Managing Information – Cybersecurity' training for all staff.
- A new Foreign Engagements Hub on the University website has been created, designed as a central information portal for all matters relating to foreign interference and influence. It houses a range of resources and information for staff.
- In 2020-21, information relating to 'Responsible Research', including matters of foreign interference, has been delivered at a number of Staff and Graduate Researcher induction and orientation events.

Due diligence, risk assessments and management

- The Office of Research Ethics and Integrity 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. Overseen by the Associate Director, Research Governance & Quality, roles such as the Export Controls Officer, the Biosafety and Biosecurity Officer, and the Program Manager Clinical Trials support implementation of the University's framework for managing export controls and sanctions, work to ensure research-related risks are appropriately managed, and that the full circumstances of any proposed research funding are understood before being accepted.
- Initiatives are underway in the Office of Research Ethics and Integrity to optimise sanctions compliance, including formal documentation of an institutional compliance action plan for sanctions; proactive review and targeted outreach to embed sanctions compliance in relevant processes, including to Graduate Researchers and Supervisors; and development of enhanced due diligence mechanisms, including procurement of software to enable multiple sanctions lists to be searched simultaneously.
- 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 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.

To supplement these principles and ensure robust academic oversight, a strengthened due diligence review process was adopted, as well as the establishment of the Research Due Diligence Advisory Group (RDDAG).

- Chaired by the Deputy Vice-Chancellor (Research), the RDDAG is an oversight and advisory group which provides process review and point of escalation on research due diligence and related risk matters. It considers emerging and potential risks, including any potential or perceived foreign influence, interference and/or security threat risks, at either sector or country level. It brings together key senior stakeholders from across the University from areas such as Legal and Risk, University Council, Academic Board, Government Relations and Academic Divisions. Critically, it has brought together different areas of the institution, such as Research and Advancement, to capture risk related processes and matters that might arise in different contexts to ensure a co-ordinated and whole-of-institution response.

  Membership of the University's Research Due Diligence Advisory Group has been extended to include a University Council member who also sits on the University's Gifts Committee (along with university staff on both) to ensure oversight and consideration of donor due diligence that may overlap with research due diligence matters

- In 2019, Research Grant and Contract Services (RGCS) established a Research Due Diligence function that advises University staff of the reputational risks associated with entering research agreements with external partners. Reputational due diligence comprises the assessment of integrity, governance, social responsibility, political and security risks.

- RGCS has implemented processes to screen and assess research projects and agreements for notification under the Foreign Arrangements Scheme and registration under the Foreign Influence Transparency Scheme.

- The Office of Research Ethics and Integrity and RGCS staff work in close consultation with Legal and Risk, Chancellery Research and Enterprise and Chancellery International.

- The University has embarked on the development of a comprehensive disclosure platform to enable staff to regularly report conflicts of interest, foreign engagements, paid outside work, and outside affiliations. It is anticipated this platform will be complete by the end of 2021.

Cyber security

- The Chief Technology Officer is overseeing a 5-year program (currently in year 3) to uplift cybersecurity capability across the institution to prevent, detect, and respond to cyberthreats. This program is working with stakeholders across the University to make the institution less vulnerable to cyber threats while balancing its need for openness, autonomy, and collaboration. It includes new and upgraded technologies and education materials, as well as a refresh of policies, processes, and guidelines.

- A mandatory cybersecurity e-Learning module training for all continuing and fixed-term academic and professional staff was developed and rolled out across the institution in late 2019. As of July 2021, 93% of University of Melbourne staff (professional and academic taken together) have completed the cybersecurity training module.
- The cybersecurity team has recruited an 'Awareness Lead' who is responsible for awareness and education about cyber-risks across the University. The team have implemented multiple education campaigns for staff including a print media campaign across the campus. Other activities include virtual presentations, regular publication of educational articles such as scam-warnings, the implementation of password managers across the organisation, and running phishing simulations to identify and report malicious emails. In conjunction with the cybersecurity e-Learning module, these activities are designed to increase staff awareness of common cybersecurity threats and the steps they can take to reduce their own and the University's exposure to these threats.
- The cybersecurity team at the University has conducted a threat modelling exercise and developed a controls framework aligned to the NIST Cybersecurity Framework (NIST CSF) to better inform its cybersecurity strategy and roadmap. This was developed in conjunction with internal technical and non-technical stakeholders and facilitated by an external cybersecurity consulting firm.

Knowledge Sharing

- The University has mapped the University of Melbourne's leading contacts and subject matter experts against relevant government agencies and public officials, aiming to highlight and enhance mutually supportive engagement with government on foreign interference.
- The University engages regularly with the Group of Eight (Go8) universities on issues relating to foreign interference and the Foreign Arrangements Scheme. The Go8 Global Engagement Group, chaired by the Deputy Vice-Chancellor International, regularly collaborates and shares best practice examples around management of Confucius Institutes, development of disclosure platforms and compliance with the Foreign Arrangements Scheme.