Submission to the Higher Education Standards Committee

September 2026

THE UNIVERSITY OF MELBOURNE

Strengthening Research Security and National Security expectations in the Threshold Standards

Executive Summary

The University of Melbourne welcomes the opportunity to contribute to the consultation on amendments to the Higher Education Standards Framework (Threshold Standards) to address research security and national security. University research and innovation are vital to Australia's future, generating new knowledge, addressing societal challenges and driving productivity. International collaboration is essential to this mission, particularly given that much of the world's research and knowledge is created offshore. Access to global research networks, research funding and international expertise is fundamental to Australia's capacity to innovate and remain competitive.

Universities currently operate within a complex regulatory environment, subject to multiple frameworks administered by different agencies with overlapping requirements—including the University Foreign Interference Taskforce (UFIT) Guidelines, ARC funding requirements, the Foreign Arrangements Scheme (FAS), Defence Trade Controls and sanctions policy. We are committed to managing the risks associated with international engagement and recognise the need for the sector to work closely with government.

Research security and cyber security are fundamentally matters of national security rather than higher education quality assurance. The University believes that these issues are more appropriately addressed through dedicated frameworks and mechanisms such as UFIT, rather than through the Threshold Standards. However, if the Government decides to amend the Standards, the following issues should be considered.

Significant changes are currently underway, including a refresh to the UFIT Guidelines and recent amendments to the Foreign Arrangements Scheme relating to researcher-to-researcher activity. These developments underscore the importance of carefully coordinating any new requirements in the Threshold Standards so they form mutually reinforcing arrangements and avoid creating inconsistent or overlapping obligations.

We note that in other areas of regulation, overly prescriptive compliance requirements have prevented universities from integrating obligations into existing governance, risk and assurance frameworks. This has forced the creation of duplicative processes and compliance-focused activity without necessarily improving substantive outcomes. Given the multiple changes currently underway, there is a particular risk that similar outcomes could occur in addressing research security.

Should the Government proceed with amendments to the Threshold Standards, new Standards should contribute to a coherent national framework for existing obligations, rather than creating a parallel compliance regime. UFIT should be the primary mechanism through which Government and the sector address research security challenges. For example, the sector is developing a framework for researcher-to-researcher collaboration through UFIT.

If new Threshold Standards are introduced, they should be principles-based and proportionate, focused on governance, accountability, and assurance outcomes rather than prescribing practices, committee structures or organisational arrangements. Universities vary in size, complexity, international footprint and research profile and should retain flexibility as to how those outcomes are achieved. Standards should be verifiable and achievable, covering matters universities can control and which TEQSA can assess, including by referencing other arrangements such as UFIT, sanctions laws and FAS. This approach will enable universities to manage risks while preserving the relationships that strengthen research—ultimately benefitting Australia more broadly.

For further information or to discuss this submission, Professor Mark Cassidy, Deputy Vice-Chancellor (Research) can be contacted at dvc-research@unimelb.edu.au.

1. **How might current assurance mechanisms be strengthened to support providers identify, assess, manage and mitigate research security, cyber security and national security risks, while appropriately supporting and protecting staff and research students and other university-affiliated or visiting staff engaged in those activities?**

Existing measures

The University has processes for monitoring research activities, scrutinising partnerships and collaborations and is proactive in managing potential risks to national interests arising from foreign interference and undue foreign influence. Globally, the research sector has experienced an increase in foreign engagement risks due to geopolitical disruption and facilitated by advances in AI and cyber.

The University's Office of Research Ethics and Integrity (OREI) provides the University's central research security capability, delivering across four risk and compliance domains: governance and oversight; awareness, support and training; risk assessment and risk management; and monitoring and review. Research activities generally present the highest risks, but to ensure compliance with the legislative obligations, OREI also provides support and oversight of non-research activities.

Research security and foreign interference risk is overseen primarily through two committees (one on research due diligence and one on geopolitical risk), reporting into the Risk Management and Compliance Sub-Committee, University Executive and the Audit and Risk Committee of University Council. These committees, chaired by the relevant Deputy Vice-Chancellors, consider emerging risks and specific proposed research engagements where there are risks of foreign interference.

Below the committee level, there are other mechanisms for governance and oversight of compliance and risk for research security and foreign interference. For example, the University has an established Foreign Interest Disclosure (FID) Program, now in its fifth year of operation. Disclosures are sought across the entire University. The results of the institutional risk assessment of all disclosures are reported through to the Audit and Risk Committee. All Deans are made aware of the specific risks in their faculties and senior leadership support is sought to help mitigate risks where necessary.

The University maintains a risk-based cybersecurity program aligned to industry standard frameworks, with controls covering governance, identity and access management, security monitoring, endpoint protection, threat detection, incident response, vulnerability and patch management, third-party risk, data protection, awareness and many others.

Possible changes

<u>Principles and proportionality</u>

If the Government decides to create new Standards, they should be principles-based and focused on outcomes rather than prescriptive technical requirements, which quickly become outdated. For example, Standards could require providers to:

- develop and maintain policies and governance frameworks that promote and uphold research security and cyber security, with clear ownership and escalation pathways for identified risks
- have in place processes to raise awareness and provide guidance on research security and cyber security within their communities
- establish monitoring and review mechanisms to track research security and cyber security risks, including through Foreign Interests Disclosures.

Any Standards should be proportionate, acknowledging that a large research-intensive university with complex international partnerships will have a different risk profile to a smaller provider with limited research activity.

Clarity and measurability

Clarity of drafting will be important. Concepts such as "research security", "national security" and "cyber security" are increasingly interconnected but do not necessarily have clear boundaries. Any new Standards should articulate what level of risk or concern triggers governance or assurance requirements, and how these concepts interact. Any resulting Standards should be sufficiently clear, measurable and capable of objective assessment by universities and regulators alike. They should be aligned with the UFIT approach.

TEQSA should consider articulating what good institutional governance looks like in practice—including governing body oversight, executive accountability, clear allocation of risk ownership, escalation pathways, internal reporting and review—through Statements of Regulatory Expectation and Guidance Notes, aligned with UFIT, FAS and other regulatory requirements. TEQSA should also issue guidance on the evidence providers will be required to produce to demonstrate compliance. Such clarity will support consistent implementation across the sector.

Ensuring Standards can be implemented and assessed

When drafting Standards that relate to research security, consideration should be given to how compliance will be assessed and how institutions will demonstrate assurance over time. Standards should be written in such a way that existing enterprise risk management, governance and assurance frameworks—including those established to meet UFIT, FAS and other requirements—can be leveraged to support compliance. We have seen in other areas of regulation that prescriptive requirements preventing such integration create duplicative, parallel compliance processes. These parallel processes divert institutional resources and attention from substantive risk management activities without necessarily improving outcomes or reducing actual risk.

2. **Are there existing legislative, regulatory, funding or sector frameworks, including ARC funding requirements, UFIT, national security obligations and other research governance mechanisms, that should be taken into account in developing any new or clarified expectations? If so, how should those expectations be framed to avoid unnecessary duplication and support effective implementation?**

While research security should ideally be addressed through dedicated frameworks, we recognise the Government may determine that amendments to the Threshold Standards are warranted. On that basis, the following observations address how such amendments could be coordinated with existing frameworks.

As noted in the consultation paper, universities are currently subject to several regulatory frameworks on research security, national security and cybersecurity, including:

- *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* (FAS)
- *Autonomous Sanctions Act 2011*
- *Foreign Influence Transparency Scheme Act 2018* (FITS)
- *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*
- ARC Research Security Framework
- UFIT Guidelines
- Defence Export Controls
- Defence Industry Security Program (DISP) where a university is an authorised member
- Safeguarding Australia's Military Secrets Program (SAMS).

Additionally, we note that the Government recently amended FAS to require universities to maintain policies and procedures for identifying research projects that involve researchers "employed or engaged by foreign entities," assessing whether those projects adversely affect the national interest or foreign policy and managing those risks. The Government is also working to refresh the UFIT Guidelines in parallel. These developments underscore the importance of ensuring that new Standards are carefully coordinated to avoid creating inconsistent or overlapping obligations and drafted in such a way that they do not require frequent updates.

One of the drafting principles for amendments to the Threshold Standards is that "amendments should not replicate obligations found in other legislation or regulation … but should reinforce those obligations." New Standards should therefore act as an integrating layer that clarifies the institutional governance and assurance outcomes expected of providers, while recognising that many of the underlying operational obligations already sit elsewhere. They should create coherence across existing research security, cybersecurity and national security obligations, rather than creating a parallel regime.

To support this approach, alignment between HESC, TEQSA, Education, Home Affairs, Defence, DFAT, ARC, NHMRC and other relevant government agencies will be important in avoiding duplication, inconsistent obligations and overlapping assurance requirements. Given the specialist nature of research security and cybersecurity risks and TEQSA's existing regulatory responsibilities and resource constraints, Standards should be designed to enable TEQSA to assess the veracity of institutional governance and assurance processes rather than requiring TEQSA to evaluate substantive security judgments. Coordination and detailed guidance on research security policies should principally remain the responsibility of UFIT.

3. **What implementation challenges, risks or unintended consequences should HESC consider in developing advice on potential amendments to the Threshold Standards, and what measures could support effective, proportionate and risk-based implementation across the sector?**

Government support

Universities have primary responsibility for managing research security and cybersecurity risks within their institutions through internal governance frameworks and regulatory requirements. However, universities cannot make fully informed risk assessments without access to relevant government information. For example, under FAS, universities have encountered situations where they lack the intelligence or foreign policy context necessary to assess whether a foreign university has "institutional autonomy." This information asymmetry undermines institutional decision-making and creates compliance uncertainty.

To address this, it is important that the Government provides universities with practical guidance on implementing any new Standards, as well as unclassified threat briefings and sector-wide alerts on emerging foreign engagement risks. UFIT remains important to this effort. Support could mirror that provided to universities in the UK or Canada. For example, the Government could develop resources similar to Trusted Research provided by the UK National Protective Security Authority. The Government could also establish an advisory point of contact, similar to the UK's Research Collaboration Advice Team (RCAT), to provide timely, confidential, and authoritative advice on national security risks linked to international research. Sufficient lead time should also be provided for universities to implement changes, including new IT systems where appropriate.

Balancing risk management with research collaboration

It is important that implementation does not create unnecessary friction or administrative burden for legitimate research collaboration. Research security should help researchers collaborate safely, not create a compliance model that slows or deters low-risk collaboration. International collaboration remains essential to Australia's universities' research missions. Standards should support informed risk management rather than discourage international engagement to ensure that Australian universities are not placed at a disadvantage relative to international competitors. This could have downstream impacts on Australia's innovation and productivity and undermine Australia's national interests.

Unintended consequences from regulatory overlap

In considering implementation challenges, HESC should consider the risks of inconsistent government expectations, overlapping reporting obligations, compliance uncertainty and increased administrative burden without a corresponding reduction in risk. These risks are particularly acute given the existing density of regulatory obligations required of universities. We note that the Better Regulation Working Group is currently considering opportunities to streamline regulation and reduce unnecessary compliance burden. It is important that new administrative burdens do not duplicate what is better delivered through other arrangements.

In summary, should the Government determine that amendments are necessary, we recommend that new Standards are high-level and principles-based, reinforcing existing obligations rather than creating a parallel compliance regime. This should be accompanied by greater guidance on what good institutional governance looks like in practice. This should complement responsible agencies providing timely, confidential and authoritative advice on national security risks linked to international research. UFIT should remain the key body through which Government and the sector address emerging risks.

The University of Melbourne

Grattan Street, Parkville, Victoria 3010 Australia

t 13 MELB (13 6352)

+61 3 9035 5511 (International)

unimelb.edu.au

THE UNIVERSITY OF MELBOURNE