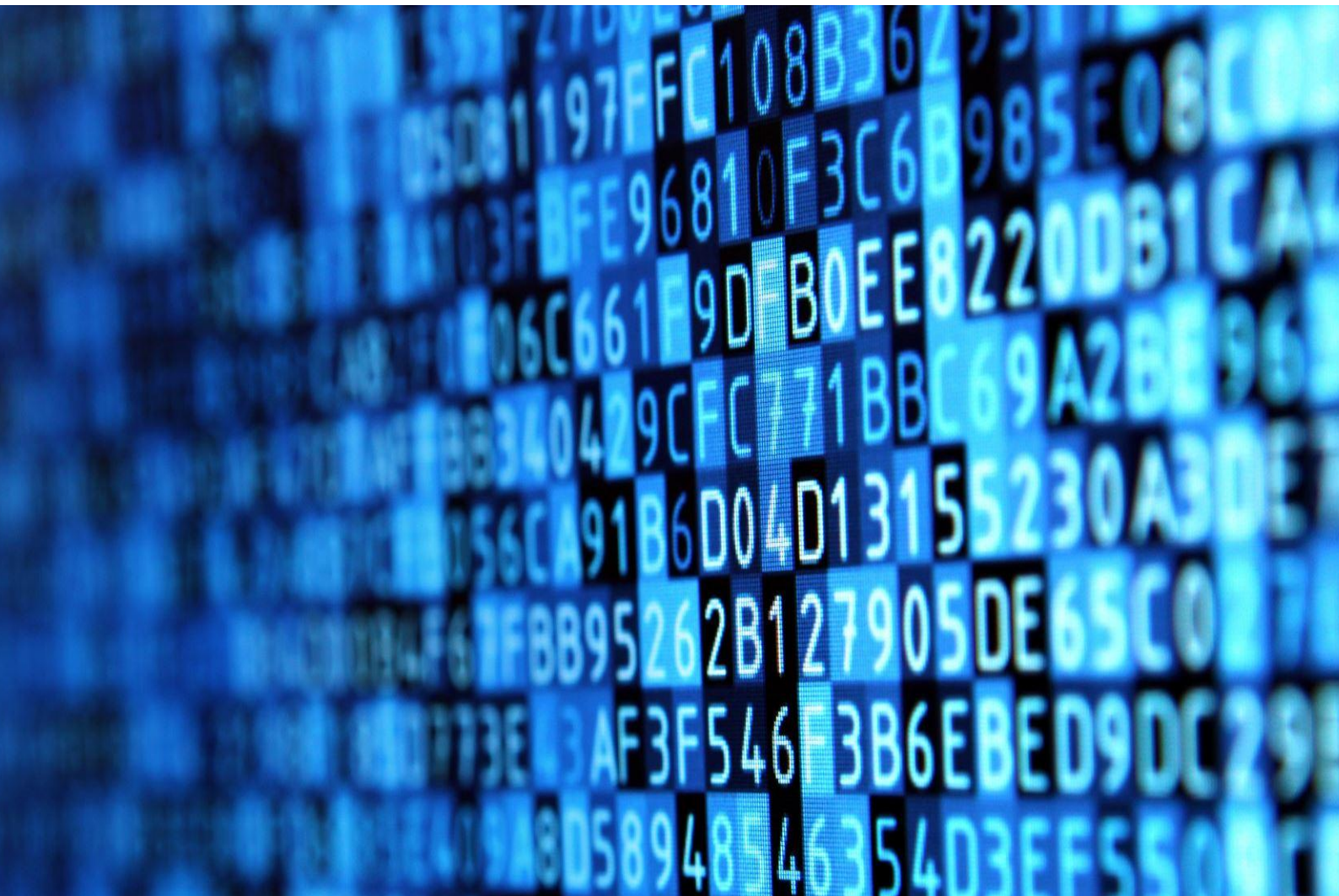
Strengthening Research Security and National Security expectations in the Higher Education Standards Framework (Threshold Standards)

Higher Education Standards Committee Consultation Paper



Strengthening Research Security and National Security expectations in the Higher Education Standards Framework (Threshold Standards)

The Hon Jason Clare MP, Minister for Education, wrote to the Interim Australian Tertiary Education Commission (ATEC) seeking advice and recommendations from the ATEC on how Australia's higher education settings can be strengthened by incorporating clear, proportionate research security and national security governance expectations into the Higher Education Standards Framework (Threshold Standards). ATEC has sought independent advice from the Higher Education Standards Committee (HESC), a statutory committee established under the ATEC, to inform its consideration of these matters. HESC is consulting with interested parties to support the development of its advice to ATEC.

HESC is seeking evidence and stakeholder perspectives to inform its advice to ATEC on how research security and national security governance could be reflected within the Threshold Standards. In particular, HESC is seeking views on the institutional governance, capability and assurance arrangements that support effective management of research security and national security risks, and on how any expectations could be implemented in a manner that is proportionate to the diversity, scale and risk profile of higher education providers. Stakeholder views are also sought on practical implementation considerations, including regulatory impacts, compliance burden, support requirements, potential benefits and any unintended consequences associated with different approaches. For the purposes of this paper, references to national security considerations include cyber security and foreign interference risks relevant to the conduct of research and the protection of research-related systems, data and intellectual property.

Context

Higher education providers form an important part of Australia’s broader research and innovation system, with public universities predominantly generating new knowledge, undertaking a substantial share of the nation’s research and development activity, and contributing to economic, social and scientific advancement through discovery, collaboration and innovation. However, Australian universities operate within an increasingly complex environment in which openness and global collaboration, while essential to academic excellence, concurrently generate exposure to security risks including foreign interference, unauthorised access to, misuse of, or compromise of research, data and intellectual property.

Australian public universities undertake the majority of publicly funded research in Australia, other registered higher education providers may also undertake research activities, including research training and applied research. The nature and extent of these activities, including collaboration with external partners, can vary between providers. While risk profile of these activities may differ across providers, research security considerations including cyber security and protection of data, systems, intellectual property and research outputs remain relevant wherever research is conducted.

The current and evolving threat landscape facing Australia's higher education sector raises questions about whether current guidance, policy settings and regulatory expectations provide sufficient clarity, consistency and assurance for contemporary research environments. While the current Threshold Standards emphasise governance, accountability and quality assurance, across all aspects of a provider's operations they do not expressly articulate minimum institutional capabilities for safeguarding research data, intellectual property (IP), and research-related systems and infrastructure in the context of research security and national security risks.

Research Security and Academic Freedom

In considering whether greater clarity is needed in relation to research security and national security expectations, it is also important to consider how these expectations interact with established principles and obligations within the higher education sector. Academic freedom remains fundamental to Australia's higher education and research system and underpins open inquiry, the advancement of knowledge, and domestic and international collaboration. Consideration of research security is not intended to diminish the importance of academic freedom or legitimate research, limit open inquiry, or reduce the value of collaboration. Academic freedom and research security are not at odds; rather, both operate within a broader legal and regulatory environment that establishes rights, responsibilities and safeguards. While academic freedom is fundamental, it does not remove institutional or individual obligations to comply with applicable laws and regulatory requirements, including those relating to sanctions, export controls and foreign interference. Research security expectations may support greater awareness and understanding of the relationship between these obligations and the exercise of academic freedom. Greater clarity regarding these relationships may assist institutions and researchers to navigate emerging research security challenges while maintaining confidence in open inquiry, international collaboration and responsible research practice.

University Foreign Interference Taskforce Guidelines to Counter Foreign Interference

The University Foreign Interference Taskforce Guidelines to Counter Foreign Interference in the Australian University Sector[1](the UFIT Guidelines) provide the primary sector-wide framework for managing foreign interference and research security risks. The Guidelines emphasise governance, due diligence, cyber security, awareness and risk management measures, while recognising that implementation should be proportionate to institutional scale, research intensity and risk profile. Universities are at the leading edge of policy, research and scientific development, making them attractive targets for malign foreign interference and other research security threats. The potential compromise of sensitive research and intellectual property carries significant consequences for Australia and for the reputation of the Australian higher education sector, including economic loss, reputational damage and broader strategic harm.

Research-related risks

Research-related risks can arise through formal institutional partnerships, researcher-to-researcher collaboration, whether domestic or international, industry engagement, data sharing arrangements and other forms of research activity. These examples raise questions about whether current arrangements provide sufficient visibility, consistency and assurance in relation to research security

[1] Guidelines to Counter Foreign Interference in the Australian University Sector

risks, including where research outcomes, expertise or technology may be applied in ways that are inconsistent with Australia's national interests.

Research-related risks may also arise through researcher-initiated activities that occur outside formal institutional partnership arrangements, including academic networking, conference engagement, advisory activities, consulting arrangements, individual collaborations, data sharing and other forms of self-directed research activity. These characteristics distinguish universities from many other research-performing organisations and raise questions about how institutional governance and support arrangements can assist researchers to identify and manage research security obligations in the course of their work.

Problem to be addressed

It is important to consider if existing mechanisms provide sufficient clarity, consistency, accountability and legal effect to assure government and the public that research security and national security risks are being managed proportionately across providers.

Australia's universities operate in an increasingly complex and competitive research environment. To balance collaboration and threat Australian universities have undertaken substantial work to strengthen their institutional resilience, transparency and safeguards against foreign interference, including through implementation of the UFIT Guidelines and related institutional governance, disclosure and risk management processes.

These considerations are relevant not only to institutional governance, but also to the protection and support of researchers themselves. Increasingly complex requirements relating to sanctions, export controls, foreign interference and international engagement may create uncertainty for researchers where institutional guidance, training and support arrangements are inconsistent. This raises questions about whether clearer institutional expectations could assist researchers to understand and manage these obligations while continuing to engage in legitimate research activity and collaboration.

While Universities receive the majority of public funding, research is undertaken by a diverse ecosystem of organisations[2] operating under different governance, security and regulatory frameworks. Consideration of any amendments to the Threshold Standards should therefore take account of the broader research ecosystem and the extent to which regulatory expectations are aligned, complementary and proportionate.

Consideration is need about the role of the Threshold Standards in establishing a sector-wide baseline of expectations for institutional capability, governance and assurance, while operating in conjunction with existing national security frameworks, funding-related requirements, guidance and sector-led arrangements.

In considering this question, HESC will also have regard to how any changes to the Threshold Standards could operate effectively and proportionately alongside other mechanisms, such as

[2] Organisations include but are not limited to Commonwealth research agencies, medical research institutes, cooperative research centres, vocational education providers, industry, and private research organisations.

strengthened guidance, implementation support, clearer government expectations, enhanced coordination, targeted regulatory amendments, or a combination of these approaches.

Issues

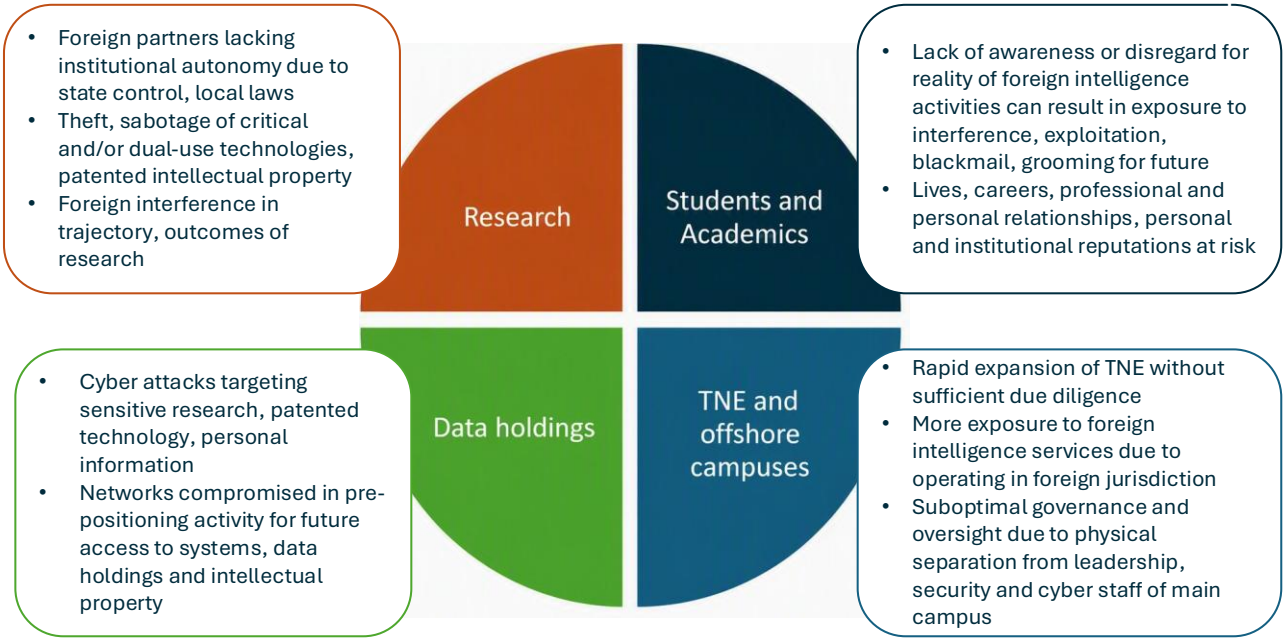
Threats to institutional and national security and existing measures

Australia's research system is central to national capability, economic growth and security. Protecting research from theft, misuse, compromise and interference is therefore an important public policy concern and a relevant consideration for institutional governance and assurance.

Public reporting by Australian security agencies indicates that espionage and foreign interference risks remain significant and are increasingly relevant to science, technology and other areas with both civilian and military applications. These risks are relevant to universities because of the scale and value of their research, data, intellectual property, infrastructure and international collaboration.

The Australian Security Intelligence Organisation (ASIO) has warned, through public reporting and engagement with the sector, that Australian higher education and research institutions may be targeted by espionage and foreign interference activities from a range of actors.

Image 1: Security threat vectors and risks facing Australian higher education



The evolving geostrategic environment, including the increasing importance of emerging technologies such as artificial intelligence and quantum technologies, has sharpened attention on whether current settings and provider governance provides sufficient assurance that research security and national security risks are identified, assessed and managed in a proportionate and effective way. Although the Threshold Standards require providers to have effective governance and risk management systems, including oversight of research activities and integrity, questions remain as to whether these arrangements adequately address emerging research security risks.

Commonwealth research funding arrangements have also evolved to include additional mechanisms for assessing security, defence and international relations risks. In 2024, amendments were made to the *Australian Research Council Act 2001* (ARC Act), including the conferral of a non-delegable Ministerial power to refuse funding applications on the basis of the security, defence or international relations of Australia. Since then, the Australian Research Council (ARC) has applied earlier security screening and reinforced disclosure requirements for National Competitive Grants Program (NCGP) funding schemes opening after 1 July 2024.

The ARC has also developed the Research Security Framework[3] (the Framework), released in May 2026, to support implementation of these arrangements. The Framework sets out how the ARC identifies and manages risks relevant to security, defence and international relations across the lifecycle of NCGP grants and articulates expectations of universities and researchers in areas such as risk assessment, disclosure of foreign affiliations and interests, and ongoing oversight.

These arrangements form part of the broader policy environment for managing national security risks in research funding. They are directed to ARC-funded research and sit alongside other mechanisms that seek to identify risks earlier, support risk-informed decision-making and maintain confidence in Australia's research system. Because not all research undertaken by registered higher education providers is funded through ARC or National Health and Medical Research Council (NHMRC) programs, consideration of the Threshold Standards focuses on how funding-related requirements interact with institution-wide governance expectations, and whether additional clarity or assurance is needed in relation to institutional systems, capability and oversight.

The University Foreign Interference Taskforce (UFIT) was established in 2019 as a forum for collaboration between government and the university sector on foreign interference risks. The UFIT Guidelines, continue to provide an important voluntary framework supporting institutional governance, due diligence and resilience measures. UFIT is currently undergoing a strategic refresh, with the aim of providing more frequent and clearer guidance to the sector on government expectations and enabling discussion of sensitive and complex national security and foreign policy risks. HESC notes that any regulatory expectations within the Threshold Standards would need to complement, and not duplicate, existing obligations, frameworks and guidance, including the implementation and functions supported through UFIT.

Universities are also expected to conduct research in accordance with the Australian Code for the Responsible Conduct of Research 2018, which establishes principles and responsibilities for institutions and researchers in maintaining research integrity within a broader legislative, regulatory and policy environment. Responsibility for research security is often dispersed across multiple operational areas within institutions, as a result, institutions may vary in their capability to identify covert foreign interference risks, assess complex ownership and control structures, and distinguish legitimate international collaboration from higher-risk activity. These factors suggest that any amendments to the Threshold Standards would need to be framed with regard to existing guidance, specialist support and government engagement, so that expectations are capable of effective and proportionate implementation. HESC is seeking views on whether existing arrangements collectively provide sufficient assurance, or whether the absence of a sector-wide, enforceable baseline creates gaps that warrant further consideration. The scope of this consultation remains focused on whether amendments to the Threshold Standards are warranted and, if so, how they should be framed.

[3] ARC Research Security Framework

Australia's universities compete internationally for talent, research partnerships, investment and funding. While effective research security arrangements can strengthen confidence and support collaboration, additional compliance, reporting or approval requirements may impact institutional agility and increase operational costs. Consideration of any amendments should therefore balance security objectives with the benefits of openness, collaboration and competitiveness.

Institutional and national preparedness for Cyber Security Risks

Australian Government reporting indicates that malicious cyber activity targeting Australian organisations is increasing in frequency, scale and sophistication. Australian Signals Directorate (ASD) reporting highlights that state-sponsored actors and cybercriminals continue to target networks across government, critical infrastructure and business to conduct espionage, steal sensitive information and enable disruptive activity. ASIO has also identified universities, academia and research centres as potential targets of cyber espionage, particularly where they hold research data, methods, concepts or dual-use technologies with both civilian and military applications. While the nature and scale of research activity varies across providers, cyber security risks can arise wherever sensitive information, research systems, proprietary knowledge or externally funded research are held or processed. Accordingly, any proposed cyber security-related amendments are likely to be relevant to all providers, irrespective of the scale or intensity of their research activities.

These reports emphasise that cyber threats are evolving and that effective mitigation requires continuous adaptation and coordinated responses across government and non-government sectors. While universities are not always identified as a distinct category in ASD reporting, the relevant threat vectors apply to organisations holding sensitive information, research data and valuable intellectual property. Available estimates of the costs of cyber security incidents and related compromise indicate that the potential consequences for higher education providers may be significant, regardless of the scale of their research activities.

Cyber incidents can also affect trust in an institution’s ability to protect student, staff and research data and information assets, as well as critical systems. Potential impacts may include disruption to research activity, reputational damage, reduced confidence among partners, and economic consequences associated with lost intellectual property, reduced collaboration or remediation costs.

Other Australian Government and sector-led analysis highlights that universities hold significant volumes of sensitive data, intellectual property and research capability, and identifies opportunities to strengthen institutional preparedness, threat intelligence sharing and workforce capability in response to evolving cyber risks[4,5].

The UFIT Guidelines identify cyber security as one of four core pillars of institutional resilience, alongside governance and risk frameworks, communication, education and knowledge sharing, and due diligence, risk assessment and management. The Department of Education’s 2023 review of UFIT implementation indicates that universities are engaging with the Guidelines, with implementation occurring to varying degrees of maturity and in ways that are proportionate to institutional risk. This variation in implementation maturity remains relevant when considering whether minimum outcomes-based expectations should be articulated through the Threshold Standards.

[4] Enhancing Cyber Security Across Australia’s University Sector: Final Report - Department of Education, Australian Government

[5] Enhancing Cyber Security Across Australia’s University Sector - RMIT University

Australian Government guidance on the cyber security pillar of the UFIT Guidelines highlights that universities must manage complex digital environments, identify critical data and systems, and implement proportionate controls to mitigate risk. The guidance notes that the complexity and openness of university networks, particularly in research-intensive environments, create challenges in protecting assets consistently and require risk-based prioritisation of cyber security efforts. ASD also provides resources, including the Information Security Manual, the Blueprint for Secure Cloud, the Essential Eight mitigation strategies, advice on modern defensible ICT architecture, operational technology for critical infrastructure, AI and quantum, and ad hoc threat advisories. ASD's Australian Cyber Security Centre also undertakes ongoing outreach to the university sector.

Taken together, the available material suggests that cyber security risks increase with reliance on interconnected digital systems, increasing volumes of sensitive information, and the growing importance of digital platforms for teaching, administration and research. While the nature and extent of these risks may differ according to institutional size, complexity and research profile, the available evidence raises questions about whether the existing provisions of the Threshold Standards provide sufficient assurance regarding cyber security governance, capability and oversight across the sector.

Research Security within the wider regulatory framework

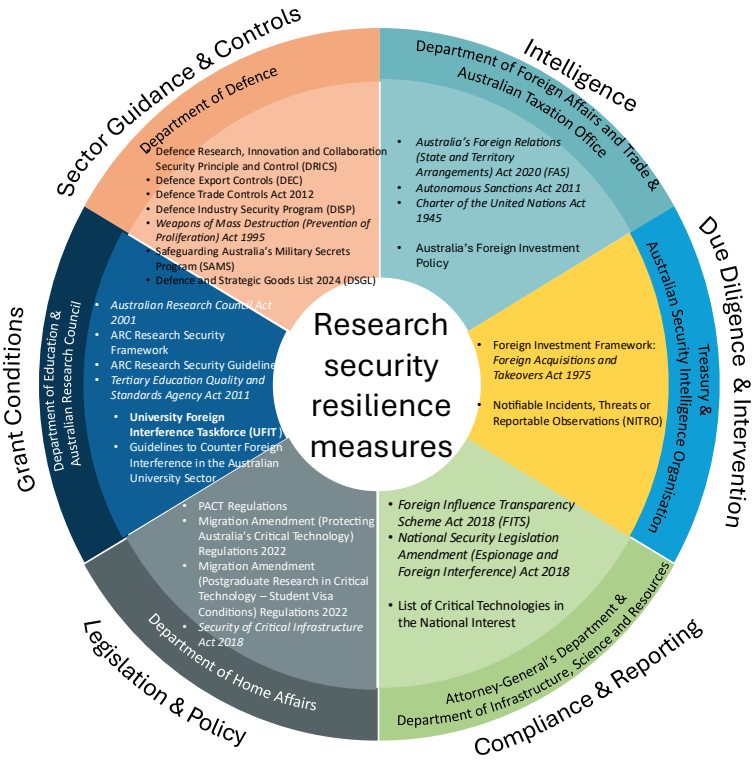
Research security, cyber security, data management and information security obligations relevant to universities are already supported through a range of existing legislative, regulatory and policy mechanisms. The *Foreign Relations (State and Territory Arrangements) Act 2020* establishes the Foreign Arrangements Scheme, requiring notification (and in some cases approval) for certain arrangements with foreign entities. The Foreign Arrangements Scheme is administered by the Department of Foreign Affairs and Trade (DFAT) and was enacted to ensure international collaborations and engagements safeguard Australia's national interests and are consistent with Australia's foreign policy settings. Further, international collaborations and engagements are also subject to sanctions laws, including the *Autonomous Sanctions Act 2011* (and associated regimes), with DFAT guidance specifically addressing sanctions compliance risks for universities.

Consideration of research security issues is also occurring across multiple Commonwealth portfolios and entities responsible for industry, science, research, trade, defence, cyber security, foreign affairs and national security. Any amendments to the Threshold Standards would therefore form one element of a broader whole-of-government approach to strengthening research security arrangements across Australia's research and innovation system.

Universities are one part of Australia's broader research and innovation system. Other research-performing organisations, such as Commonwealth entities including CSIRO, medical research institutes, cooperative research centres and private-sector research organisations, are subject to different legislative, governance and security arrangements. While many obligations relating to integrity, research security, cyber security and risk management overlap, they are not identical. This raises questions about the extent to which new requirements within the Threshold Standards would align with, complement or diverge from expectations applying elsewhere in the research ecosystem.

In addition to the Foreign Arrangements Scheme, research activity may also trigger Australia's export controls, including obligations under the *Defence Trade Controls Act 2012* in relation to controlled technology and the Defence and Strategic Goods List, or the *Security of Critical Infrastructure Act 2018*, where research is categorised as a critical infrastructure asset.

Image 2: National resilience, transparency and CFI measures (full page image at page 12)



Together, these legislative, regulatory and policy mechanisms form a significant part of the national architecture for managing research-related national security risks. Against this backdrop, consideration of the Threshold Standards should focus on the extent to which institutional governance arrangements support effective oversight, risk management and assurance across the institution.

The Threshold Standards and Quality Assurance

Existing arrangements relevant to research security are diverse and include legislative, funding, advisory and sector-led mechanisms. While these arrangements contribute significantly to risk management, their scope and application vary. The question for consultation is whether the Threshold Standards should also articulate minimum outcomes-based expectations for institutional governance, capability, competitiveness and assurance relating to research security and national security risks, and if so, how such requirements could complement existing frameworks without creating unnecessary burden or duplication.

Any proposed regulatory change should also have regard to implementation impacts and administrative burden. New governance, reporting, training or assurance requirements may impose direct and indirect costs on institutions, researchers, students and professional staff. Any amendments would therefore need to demonstrate a clear public benefit and support a proportionate and risk-based approach to implementation.

International Settings

International experience illustrates a range of approaches to research security, including advisory services, funding conditions, legislative mechanisms, guidance and specialist implementation support. The United Kingdom established the Research Collaboration Advice Team (RCAT), which sits within the Department for Science, Innovation and Technology (DSIT). RCAT is a resource for research institutions seeking clarification to support adherence with specific legislative requirements or policy guidance. In limited cases, RCAT assists institutions to assess risks around specific collaborations. Research institutions are not required to consult RCAT, and alignment with RCAT advice is voluntary. RCAT was established to meet demand in the academic research sector for clear advice from government on the changing research security landscape.

The United Kingdom also has UK Research and Innovation (UKRI), which established a Trusted Research and Innovation team to provide guidance and support to the sector in managing risks associated with global research and innovation collaboration. The United Kingdom is also developing its first research security strategy, which is expected to underpin the work of RCAT, and has a suite of national security legislation relevant to research security.

Canada has established the Research Security Centre to support implementation of the National Security Guidelines for Research Partnerships (NSGRP), providing a coordinated national approach through funding conditions, risk assessments, government guidance and specialist security expertise. The Centre assists with additional national security screening where needed and provides centralised guidance to funding councils on security considerations relevant to funding applications. The Research Security Centre is also a point of contact for Canadian researchers and universities seeking support to safeguard their research. The NSGRP requires research institutions applying for certain types of funding from the three main funding councils to complete a national security risk assessment form where a private entity is one of the counterparties in the research partnership. Canada has also developed sensitive technology and named research organisation lists through its STRAC policy and has a suite of national security legislation.

Consideration of international approaches assists in understanding how comparable systems manage research security risks while preserving openness and collaboration. In addition to Canada and the United Kingdom, developments within the European research and innovation system include research security measures associated with Horizon Europe and the European Union's broader research security agenda. These initiatives illustrate the range of tools governments and research institutions may use, including advisory, funding-linked, guidance-based, coordination and regulatory mechanisms. The range of approaches suggests that reliance on a single mechanism may present challenges in achieving consistency, clarity and assurance across the sector, and raises a question about whether complementary mechanisms, including potential regulatory mechanisms, may be warranted. Against this backdrop, existing legislative, regulatory and policy mechanisms provide a relevant foundation, but may not consistently establish a sector-wide enforceable baseline for institutional capability.

Amending the Threshold Standards

Recent consultation undertaken through the former Higher Education Standards Panel's review of emerging technology risks, including generative artificial intelligence, highlighted the importance of robust institutional governance, risk management, information security and oversight to ensure higher education providers can effectively manage the evolving impacts of emerging technologies on teaching, research and institutional operations. In considering any amendments related to research security and national security, HESC is conscious of the significant consultation already undertaken across the sector and is seeking to build on, rather than duplicate, feedback received through previous reform and consultation processes. Stakeholder views are sought on whether existing Threshold Standards and recent reforms provide sufficient assurance, or whether targeted amendments are warranted.

Collectively, the current Threshold Standards provide a principles-based and outcomes-focused foundation for managing information security and integrity risks. However, they do not explicitly reference cyber security, research security or national security considerations, nor do they establish specific expectations regarding research security awareness, capability or the management of risks associated with contemporary research environments.

Part A of the Threshold Standards contains a range of provisions relevant to cyber security, personal data security and, to a more limited extent, research security. These include requirements for the secure management of information systems and records (paragraph b of Standard 7.3.3), the successful management of research partnerships (paragraph c of Standard 4.1.1), the promotion of safe environments and online safety awareness (Standard 2.3.4), critical incident management (Standard 2.3.5), the mitigation of risks to academic and research integrity (Standard 5.2.2), research integrity and accountability (Standard 5.2.4), delivery with other parties (Standard 5.4.2), and broader governance and risk management obligations (Sections 6.2 and 6.3).

In considering how research security and national security governance expectations may be reflected within the Threshold Standards, regard may need to be had to the scale, nature and risk profile of research activity undertaken across the sector. The nature and scope of any amendments to Part A would need to remain proportionate to the varying levels of research activity undertaken by different provider types. Although some non-university providers may undertake research that intersects with national security considerations, available evidence suggests that such instances are relatively uncommon rather than systemic.

Universities occupy a distinctive position within Australia's research system. They undertake large volumes of institutionally directed research, support academic inquiry across a wide range of disciplines and frequently enable researcher-initiated activity that may not be subject to the same program-level governance arrangements that apply in some other research environments. Universities also play a critical role in educating and training the future research workforce and, as such, are central to establishing research cultures and practices that are responsive to research security and national security considerations. This combination of autonomy, openness and research intensity creates both significant opportunities and unique governance responsibilities. Research security risks are also concentrated within universities due to the scale and intensity of their research activity, the presence of advanced infrastructure, and the extent of international collaboration. The Part B category standards already recognise sustained research capability as a defining characteristic of Australian Universities, distinguishing them from other provider categories.

Accordingly, consideration could be given to whether Part B provides the most appropriate and proportionate mechanism for embedding enforceable criteria and expectations aligned to the functions and risk profile of the Australian University category. Limited amendments to Part A may nevertheless assist in signalling the importance of research security as a system-wide consideration and establishing overarching expectations applicable to all providers. This would support an approach in which broad expectations are reflected in Part A, while more specific requirements are incorporated through Part B for the Australian University category.

Such an approach would maintain the differentiated intent of the Threshold Standards, avoid duplication between general and category-specific requirements, minimise unnecessary burden on lower-risk providers, and focus regulatory obligations where they are most likely to strengthen and protect the security and resilience of Australia's research system.

Within this context, consideration could be given to whether targeted amendments would strengthen institutional capability, governance and oversight in relation to research security and cyber security risks associated with university research activity. It is important that any amendments remain outcomes-based and proportionate, requiring providers to demonstrate that systems, controls and processes are fit for purpose and appropriate to the nature, scale and risk profile of their research activities, thereby preserving institutional autonomy while supporting a consistent baseline of resilience across the sector. Any amendments could also recognise that institutions have a responsibility to provide a safe and supportive environment for staff, research students and affiliated researchers by ensuring they are appropriately informed, equipped and protected from research security, cyber security and foreign interference threats arising from their work. Likewise, consideration would need to be given to how any amendments could provide a proportionate and enforceable mechanism to support research security and cyber security expectations while complementing existing guidance, funding-linked requirements and other policy mechanisms.

Consultation Questions

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?

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?

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?

Submissions are due Monday 7 September 2026 to hesc@atec.gov.au

Image 2: National resilience, transparency and CFI measures