

September 2, 2026

ACGR Response to ATEC consultation – Strengthening Research Security and National Security Expectations in the Higher Education Standards Framework (Threshold Standards)

The Australian Council of Graduate Research (ACGR) welcomes the opportunity to provide a response to the Higher Education Standards Committee (HESC) consultation on strengthening research security and national security expectations within the Higher Education Standards Framework (Threshold Standards).

ACGR is the national peak body for graduate research in Australia's higher education sector. All universities accredited by TEQSA to deliver research training programs are members of the ACGR, represented by Deans of Graduate Research and equivalent leaders from Australian universities offering Higher Degree by Research (HDR) programs. Founded in 1997, ACGR plays a leading role in promoting excellence in research and research training nationally and in positioning graduate research as a key contributor to Australia's future prosperity.

ACGR supports the objective of protecting Australia's research system from foreign interference, inappropriate foreign influence, cyber security threats and other research security risks. Australia's research capability, innovation system and international standing depend upon a research environment that is both secure and internationally connected.

ACGR also strongly supports the position that research security must be approached in a manner that preserves the openness, academic freedom and international collaboration that are fundamental to Australian research. Academic freedom and research security should not be regarded as competing objectives. Rather, effective research security should enable researchers and institutions to participate confidently in legitimate international collaboration while ensuring that appropriate risks are identified and managed.

ACGR supports the position that amendments to the Threshold Standards are not necessary at this time. Australian universities have already undertaken substantial work to strengthen research security capability through the University Foreign Interference Taskforce (UFIT) Guidelines, the Australian Research Council Research Security Framework, legislative requirements and institution-specific governance and risk management arrangements.

The priority should now be implementation, capability-building, trusted information sharing and the maturation and evaluation of existing arrangements, rather than introducing an additional layer of regulatory requirements through the Threshold Standards.

A proportionate and risk-based approach

Research security is an important institutional responsibility, but it is also an area in which risks are complex, dynamic and continually evolving. Research collaborations vary considerably in their nature, purpose, discipline, participants, technologies, data and potential national security implications. A regulatory framework therefore needs to enable institutions and researchers to exercise informed judgement rather than seek to prescribe every circumstance in which risk may arise.

The Threshold Standards are designed to provide stable, sector-wide expectations that support consistency and comparability across a diverse higher education sector. Research security, by contrast, requires flexibility, responsiveness and access to contemporary government advice. The characteristics that make the Threshold Standards effective as a quality assurance instrument are not necessarily the characteristics required for effective management of rapidly evolving national security and research security risks.

ACGR therefore supports a principles-based, outcomes-focused and risk-proportionate approach. Any expectations applying to providers should focus on whether institutions have appropriate governance, capability, support, risk management and assurance arrangements, rather than prescribing detailed operational processes.

This distinction is particularly important given the diversity of the Australian research system. Providers differ substantially in their research intensity, disciplines, international partnerships, research infrastructure and exposure to particular security risks. A proportionate approach should allow institutions to develop arrangements appropriate to their own research profile while maintaining a clear baseline of responsible practice.

Existing arrangements provide an important foundation

Australia already has a substantial yet continually evolving framework for managing research security and national security risks. This includes the UFIT Guidelines, the Australian

Research Council Research Security Framework, the Foreign Arrangements Scheme, sanctions and export control requirements, research integrity obligations and institutional governance arrangements.

The consultation paper itself identifies the significant range of existing legislative, regulatory, funding and sector-led mechanisms that contribute to research security.

In this context, ACGR considers that the central policy question should not simply be whether another regulatory requirement can be added to the Threshold Standards. Rather, consideration should be given to whether existing arrangements are being effectively implemented, whether researchers and institutions have sufficient access to advice and whether government and the sector have effective mechanisms for sharing information about emerging risks.

The recent legislative changes relating to foreign research projects further strengthen the existing framework by establishing requirements for universities to identify, assess and manage relevant risks. The policy priority should therefore be ensuring that these obligations are understood and effectively implemented across the research system.

Creating additional Threshold Standards requirements risk creating duplication across frameworks that are already subject to different reporting, compliance and assurance mechanisms. This will increase administrative burden without necessarily improving research security outcomes.

The importance of implementation and capability-building

ACGR considers that the greatest opportunity for strengthening research security lies in building the capability of researchers and institutions to identify and respond appropriately to risk.

Research security is not solely an institutional governance issue. It also depends on the decisions made by researchers in the course of their everyday work. Researcher-to-researcher engagement, international networking, conferences, collaborative publications, data sharing, advisory activities and other informal forms of scholarly engagement may occur before a proposed activity becomes visible through formal institutional processes.

Researchers therefore need to understand what constitutes a potential risk, how to recognise indicators of concern and, critically, when and how to seek advice.

This capability-building approach should extend across the research workforce and should explicitly include higher degree by research (HDR) candidates.

HDR candidates as an integral part of Australia's research system

HDR candidates are an important component of Australia's research workforce. They undertake research that contributes to institutional and national research capability and participate in many of the same research activities as academic staff, including international collaboration, publication, conferences, research placements, data sharing, access to research infrastructure and engagement with external research partners.

HDR candidates may also be at an earlier stage of developing their professional research judgement. They should therefore not be expected to independently interpret complex requirements relating to foreign interference, sanctions, export controls, international engagement, data security or dual-use research.

Instead, universities should provide HDR candidates with clear guidance, appropriate education and accessible pathways to expert advice.

Research security education should be incorporated into the broader development of HDR candidates as responsible and capable researchers. It should complement existing education in research integrity, research ethics, responsible research conduct, data management, intellectual property and research governance.

ACGR therefore supports the development of nationally consistent baseline research security education and resources for HDR candidates and researchers, supplemented by discipline-specific training where the nature of the research warrants it.

Such resources should be practical and scenario-based, helping researchers understand issues such as:

- knowing and appropriately assessing and declaring research collaborators and their affiliations;
- recognising potential indicators of foreign interference or other concerning behaviour;
- understanding obligations relating to sanctions and export controls;
- protecting research data, intellectual property and sensitive information;
- understanding potential dual-use implications of research;
- appropriately managing access to research infrastructure and capabilities;
- considering risks associated with international travel, conferences and researcher-to-researcher engagement;
- understanding when institutional advice should be sought; and
- knowing how to pause or escalate an activity where concerns arise.

The objective should be to build confidence and capability that strengthens Australia's research system by working with strategically valuable and complementary international partners rather than create an environment in which researchers become reluctant to engage internationally because of uncertainty about regulatory requirements or an inclination to avoid red tape.

Shared responsibility

ACGR strongly supports a model of shared responsibility between researchers, institutions and government.

Researchers should exercise informed professional judgement and comply with applicable laws, policies and institutional requirements. Universities should provide the systems, guidance, training, oversight and specialist support necessary for researchers to make those judgements effectively. Government should provide timely, authoritative and accessible advice about emerging national security, foreign interference, sanctions and export control risks.

This shared-responsibility model is particularly important for HDR candidates. Their capacity to manage research security risks is strongly influenced by the quality of supervision, research training and institutional support available to them.

Supervisors and graduate research leaders therefore have an important role in helping HDR candidates understand their responsibilities and identify when specialist advice is required. Research security should become part of the culture of responsible research practice rather than being viewed solely as a compliance function.

The role of UFIT

ACGR supports the continuing role of UFIT as an important mechanism for collaboration between government and the university sector on research security and foreign interference.

The current UFIT refresh provides an opportunity to strengthen sector-wide consistency, develop practical resources, share emerging intelligence and clarify government expectations.

A sector-led implementation mechanism can be more responsive than embedding detailed requirements in the Threshold Standards. It can also allow guidance to evolve as the threat environment, government policy and international circumstances change.

ACGR therefore considers that UFIT should remain central to the development of practical implementation guidance, shared tools, training resources and communities of practice.

The role of TEQSA and regulatory assurance

ACGR supports the view that caution is required in assigning TEQSA an active research security assurance role.

Research security frequently depends on contextual judgement, current intelligence and information held by specialist government agencies. TEQSA is not a national security or intelligence agency and does not independently hold the information necessary to determine whether particular collaborations, entities, technologies or relationships present national security concerns.

For TEQSA to undertake such a role would require significant additional capability and relationships with the National Intelligence Community and relevant government agencies.

There is also a risk that a new regulatory assurance role could add another layer of assurance to a system already supported by direct government–sector relationships, institutional governance and UFIT.

ACGR considers that regulatory assurance should focus on whether an institution has appropriate systems, governance and capability to manage research security risks rather than whether individual research collaborations are substantively assessed by the regulator.

Protecting academic freedom and international collaboration

Australia's research system derives significant strength from its international connectedness. The overwhelming majority of international research collaboration is legitimate, beneficial and in Australia's interests.

Research security arrangements should therefore be designed to enable secure collaboration, not restrict legitimate collaboration.

ACGR supports the principle that low-risk scholarly activity should not be unnecessarily constrained and that risk management should be commensurate with the nature and circumstances of the activity.

This is particularly important for HDR candidates, whose development as researchers depends on participation in domestic and international scholarly communities. International conferences, collaborative publications, research placements, visiting programs and engagement with international researchers are important elements of research training.

Any research security framework should therefore operate consistently with academic freedom, procedural fairness, natural justice and relevant anti-discrimination obligations.

Minimising unnecessary administrative burden

ACGR recognises the importance of institutional assurance and accountability. However, additional reporting, approval and compliance requirements will create substantial administrative burdens for institutions, researchers, supervisors and HDR candidates.

Universal reporting requirements for researcher-to-researcher engagement would be particularly problematic and could discourage legitimate scholarly interaction while generating considerable low-value administrative activity.

Institutions should have appropriate visibility of higher-risk research activity and clear mechanisms for escalation, while routine and low-risk scholarly engagement should encouraged to proceed without unnecessary administrative barriers.

Building institutional capability

ACGR supports universities continuing to develop institutional capability through:

- practical research security guidance and decision-support tools;
- clear and accessible advice for researchers and HDR candidates;
- baseline and discipline-specific training;
- appropriate specialist expertise;
- accessible escalation pathways;
- integration with research integrity, ethics, risk and governance systems;
- proportionate due diligence;
- appropriate protection of research data and intellectual property;
- continuous monitoring of emerging risks; and
- participation in sector-wide learning and capability development.

These arrangements should be subject to continuous improvement rather than treated as a static compliance exercise.

Conclusion

ACGR supports the objective of strengthening research security and protecting Australia's national interests. We also support the position that the priority at this stage should be implementation and capability-building rather than further regulatory intervention through the Threshold Standards.

Australia has already established a substantial framework for research security through legislation, funding requirements, government guidance, institutional governance and

sector-led mechanisms. The challenge now is to ensure that these arrangements are implemented consistently, understood by researchers and supported by timely government advice.

The most effective approach will be one that combines strong institutional governance with practical researcher capability, proportionate risk management, trusted information sharing and sector-wide coordination.

For graduate research education, this means ensuring that HDR candidates are explicitly recognised as participants in Australia's research system and are equipped with the knowledge, judgement and support necessary to undertake research securely and responsibly. Research security should be embedded within the broader development of capable, ethical and internationally engaged researchers.

ACGR therefore supports an approach based on shared responsibility, proportionality, informed judgement, academic freedom, trusted advice and continuous improvement.

If changes are ultimately made to the Threshold Standards, ACGR recommends that they remain high-level, principles-based and outcomes-focused. They should establish appropriate expectations for institutional governance and capability without duplicating existing requirements or prescribing operational processes that are better addressed through UFIT, government guidance, funding frameworks and institutional implementation.

Australia's research security will be strongest when researchers are supported to make informed decisions, institutions are equipped to manage risk proportionately, and government provides timely and authoritative advice. This approach will protect Australia's national interests while preserving the openness, international collaboration and academic freedom that are essential to a strong and globally connected research system