Australasian Research Management Society

Submission from the Australasian Research Management Society (ARMS) on the consultation: Strengthening Research Security and National Security Expectations in the Higher Education Standards Framework (Threshold Standards)

Introduction

The Australasian Research Management Society (ARMS) welcomes the opportunity to provide feedback on the Higher Education Standards Consultation relating to research security. As the peak body for Research Management Professionals across Australia, New Zealand (Aotearoa) and Singapore, ARMS represents a community of more than 5,000 Research Management Professionals working across universities, medical research institutes, government agencies, industry and other research organisations.

Research Management Professionals play a critical role in supporting the research lifecycle. They provide advice on research governance, grants management, research integrity, compliance, due diligence, partnerships, contracts and funding requirements. They are often responsible for implementing and operationalising research security requirements within institutions and supporting researchers to understand and meet their obligations.

ARMS supports stronger research security assurance to ensure that Australia's research system remains secure, resilient and internationally engaged. However, ARMS does not consider that the existence of research security risk, by itself, establishes the need for additional enforceable Threshold Standards. Before recommending new requirements, HESC should identify the material assurance gap that is not already addressed through existing legislation, funding conditions, policy frameworks and institutional controls. Thereafter, any changes to the Higher Education Standards Framework (HESF) should be practical, proportionate, risk-based and aligned with existing obligations. They should strengthen institutional capability without creating unnecessary duplication or additional administrative burden.

Research Management Professionals must translate requirements from multiple frameworks into workable institutional processes, often across grants administration, partnerships, contracts, research integrity, higher degree research, data management, export controls, sanctions, foreign arrangements and cyber security. Where these frameworks use different definitions, evidence requirements or reporting periods, Research Management Professionals must reconcile those differences at the operational level, increasing the risk of duplication, inconsistent advice and error. They are often responsible for interpreting these requirements, advising researchers, managing institutional assurance processes and implementing governance controls. Recent sector experience with Australian Research Council research security requirements illustrates the practical difficulties that arise when disclosure expectations are not clearly defined or are subject to differing interpretations. This experience reinforces the importance of clear, practical and nationally consistent guidance as a foundation for effective research security implementation.

ARMS' recent collaboration with Universities Australia (UA) to establish a Research Security Working Group provides a mechanism for drawing together Research Management Professionals, institutional representatives, universities and research institute networks, including representatives from INFIN, to develop practical guidance that supports greater consistency across the sector. The Working Group was formed in response to sector concerns regarding the interpretation and application of disclosure requirements, particularly in relation to Australian Research Council grant applications, Its work demonstrates the importance of practical, nationally consistent guidance that can be applied prospectively, rather than institutions being required to reconstruct and reinterpret obligations after a concern arises.

Question 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?

ARMS supports strengthening research security through a capability-focused and risk-based approach rather than the introduction of prescriptive compliance requirements.

Institutions need clear and practical mechanisms that help them identify and manage risk while continuing to support legitimate research collaboration and international engagement. Research security should be embedded within existing research governance, risk management, research integrity and cyber security processes wherever possible.

Research security assurance must be based on shared responsibility. Institutions and Research Management Professionals can assess the purpose of a collaboration, funding sources, partner information, data sensitivity, contractual protections, sanctions, export controls and potential end-use. They and their institutions cannot reliably determine matters that depend on classified threat assessments, non-public partner information or intelligence held by government. A clear pathway is therefore required for institutions to obtain timely and authoritative government advice before decisions are made.

From a research management perspective, strengthening assurance mechanisms should focus on:

- Clear and practical guidance for institutions and researchers.
- Consistent approaches to due diligence and risk assessment.
- Improved training and awareness programs.
- Better support for disclosure requirements.
- Access to shared sector resources and examples of good practice.

ARMS members consistently report that researchers can find research security obligations difficult to interpret, particularly where guidance is complex or applied differently across institutions. Confusion is most likely to arise when requirements are unclear rather than through deliberate non-compliance.

Recent ARC disclosure requirements provide a practical example of this challenge. Universities have reported difficulties determining consistently what information must be disclosed, where disclosures

should be recorded and how obligations should be interpreted across different ARC systems and time periods. Ambiguity around concepts such as appointments, affiliations, honorary positions, visiting appointments and voluntary roles has resulted in different interpretations across institutions, often without any intention to withhold information. Where assurance requests arise, institutions can be required to reconstruct historical relationships, gather evidence and make complex institutional judgements after the issue has already become a potential funding risk. This places a significant administrative burden on researchers and research offices and highlights the need for clearer prospective guidance.

The ARMS and Universities Australia Research Security Working Group was established specifically in response to these challenges. Its objective is to develop practical, sector-led guidance that supports consistent interpretation of disclosure requirements across universities, improves understanding among researchers and research administrators, and reduces the risk of inconsistent compliance outcomes. The strong level of sector participation in the Working Group demonstrates the demand for practical implementation guidance rather than additional regulatory requirements alone.

ARMS believes that strengthening capability through guidance, training and engagement will achieve better outcomes than introducing additional reporting requirements.

Recommendation

Government should work with ARMS and the broader sector to develop practical guidance, training resources and common approaches to research security due diligence and disclosure requirements. Research Management Professionals should be recognised as key contributors to the successful design and implementation of institutional research security frameworks as they will be essential to implementation. The work of the ARMS and Universities Australia Research Security Working Group provides a practical model for how government and the sector can collaborate to improve consistency, understanding and compliance outcomes.

Question 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?

Yes. Higher education providers already operate within a complex environment of legislative, regulatory and funding obligations. These include:

- Australian Research Council (ARC) funding requirements.
- National Health and Medical Research Council (NHMRC) requirements.
- Universities Foreign Interference Taskforce (UFIT) guidance.
- Export control obligations.
- Sanctions requirements.
- Cyber security obligations.
- Research integrity frameworks.
- Institutional governance and risk management frameworks.

Before introducing any additional enforceable expectation, HESC should identify the specific assurance gap that remains after existing obligations, and current institutional controls are considered. The proposed requirement should be shown to improve prevention, detection, response or recovery, be proportionate across different providers, and be capable of consistent implementation and assessment. A further attestation or reporting process should not be introduced unless it produces a demonstrable security benefit.

ARMS strongly encourages any new or revised expectations to be aligned with these existing frameworks rather than creating additional parallel requirements.

One of the challenges currently facing institutions is the increasing number of overlapping and sometimes inconsistent requirements. Research Management Professionals frequently support researchers who are required to provide similar information through multiple systems and processes. This can create confusion, duplication and increased compliance costs for both institutions and researchers. ARMS recommends a “one risk assessment, multiple uses” approach. Where substantially the same information, risk factors and controls are relevant to ARC requirements, UFIT, foreign arrangements, export controls, sanctions, cyber security or the Threshold Standards, institutions should be able to reuse the underlying assessment and evidence. Research managers should not be required to collect, translate and re-enter equivalent information across multiple frameworks solely because different agencies use different terminology or assurance processes.

The experience of implementing ARC disclosure requirements illustrates the risks associated with overlapping frameworks and differing interpretations. Research security obligations are increasingly spread across funding rules, institutional policies, foreign arrangements requirements, research integrity frameworks and broader national security obligations. In practice, researchers and institutions are often required to provide similar information through multiple systems that use different terminology, definitions and reporting periods. This creates duplication, increases compliance costs and can inadvertently introduce inconsistency into institutional decision-making.

The experience of the ARMS and Universities Australia Research Security Working Group has highlighted considerable variation across institutions in how disclosure requirements are interpreted and applied. Differing interpretations of existing guidance can create uncertainty and increase institutional risk. There is a significant opportunity to improve consistency through nationally aligned guidance and common approaches to disclosure and due diligence.

ARMS further notes that recent amendments relating to foreign arrangements and foreign research projects introduce additional obligations for institutions while key concepts, including "national interest" and the scope of relevant research projects, remain subject to interpretation. Nationally consistent definitions are particularly required for:

- research security;
- national security risk;
- national interest;
- research project;
- sensitive research;
- foreign entity;

- critical technology;
- affiliation and appointment; and
- proportionate risk management.

Clear definitions and alignment between any revised Threshold Standards and existing legislative requirements will be critical to avoid further complexity and uncertainty for institutions. Definitions should distinguish routine academic activities, including publications, conference participation, honorary roles, visiting arrangements and preliminary research discussions, from activities that create a credible national security consequence.

ARMS also believes that research security should not be viewed as a stand-alone compliance function. It should be integrated into existing governance structures and institutional assurance processes.

Recommendation

If Government determines that additional expectations are necessary, they should form part of one coherent national architecture that identifies the purpose, scope, lead agency and assurance requirements of each relevant framework. Common terminology should be used wherever possible, and evidence prepared for one framework should be reusable for corresponding obligations under another. Future research security expectations should be aligned with existing legislative, funding and governance frameworks and should support nationally consistent approaches to disclosure, due diligence and risk assessment. New requirements should avoid duplicating existing obligations and instead build on established institutional processes. Particular attention should be given to aligning terminology, reporting expectations and definitions across existing frameworks to support consistent implementation.

Question 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?

ARMS encourages HESC to recognise the diversity of Australia's higher education sector. A framework that may be appropriate for a large research-intensive university may not be suitable for smaller institutions, regional universities, specialised providers or organisations with a lower research risk profile. A principles-based approach will therefore be more effective than a highly prescriptive model.

Potential implementation challenges include:

- Variation in institutional size, capability and resources.
- Increased administrative burden on researchers and professional staff.
- Duplication of existing compliance activities.
- Inconsistent interpretation of requirements across the sector.
- Reduced willingness to engage in legitimate international research collaborations if requirements are perceived as excessively complex or restrictive.

This could lead to consequences such as:

- Reduced visibility of material risk. If requirements generate large volumes of routine disclosures and assessments, significant risks may be harder for institutions, regulators and government agencies to distinguish from low-risk activity.
- Inconsistent national implementation. Ambiguous definitions and decision thresholds may lead providers to interpret equivalent activities differently, preventing government from obtaining a reliable and comparable view of research security risk across the sector.
- Fragmented assurance. Overlapping requirements administered through different frameworks may produce multiple partial assessments rather than one coherent understanding of the relevant research, partner, technology, data and end-use risks.
- Poor targeting of government intervention. If scope is defined through broad categories such as international collaboration or critical technology, rather than credible indicators and potential consequences, government attention and sector capability may be directed towards routine activity instead of the matters presenting the greatest risk.
- Lower-quality information and reporting. Complex, repetitive or unstable disclosure requirements may produce inconsistent information across systems and reporting periods, limiting its value for government assurance, risk analysis and decision-making.
- Delayed identification and escalation of emerging risks. Where responsibilities and referral pathways are unclear, higher-risk matters may not reach the appropriate government agency early enough for informed advice or intervention.
- Risk displacement rather than risk reduction. Excessive or unpredictable controls may discourage formal collaboration or move activity to organisations or arrangements subject to less mature oversight, without reducing the underlying national security risk.
- Unintended reduction in voluntary disclosure. If researchers perceive security processes as punitive, indiscriminate or difficult to navigate, they may be less inclined to seek early advice. This would reduce the visibility on which effective government and institutional assurance depends.
- Difficulty assessing regulatory effectiveness. If success is measured through the number of disclosures, assessments or institutional controls rather than the prevention, detection, mitigation and management of material risks, government may be unable to determine whether the framework is producing better security outcomes.

For government, the central implementation risk is that additional requirements may increase the volume of assurance activity without improving the quality, consistency or timeliness of information available for national risk assessment. A poorly integrated framework could make material risks more difficult to identify, produce inconsistent decisions across providers and direct government and sector capability towards routine compliance rather than higher-risk matters. Proposed reforms should therefore be assessed by whether they improve national visibility of material risk, support timely escalation to the appropriate agency, enable consistent and well-informed decisions, and result in demonstrable improvements in prevention, detection, mitigation and response.

Research security measures should support informed decision-making and risk management, not discourage collaboration, researcher mobility or international partnerships. Australia's research system benefits significantly from international engagement, and security measures should be designed to support this while appropriately managing identified risks.

Implementation arrangements should also protect staff, research students, visiting researchers and affiliates who may be affected by research security decisions. Processes should be transparent and timely, provide clear reasons where activities or access are restricted, and include mechanisms for review or clarification. Risk assessments should focus on the nature of the research, data, technology, partner, funding, likely end-use and credible threat indicators, rather than a person's nationality, ethnicity, citizenship or ordinary international connections. Clear government guidance will be essential to support consistent, fair and evidence-based decisions across the sector.

ARMS considers capability development to be one of the most important factors in the successful implementation of any future research security requirements. Experience across the sector demonstrates that compliance outcomes improve when researchers and professional staff have access to practical guidance, worked examples, common definitions and opportunities to share good practice. The ARC disclosure environment has shown that ambiguity is often not a result of unwillingness to comply, but rather uncertainty about how requirements should be interpreted and applied in practice. Addressing these issues through capability building can improve compliance outcomes while reducing unnecessary administrative burden.

Effective implementation will require:

- Training materials.
- Sector-wide guidance.
- Shared tools and templates.
- Examples of effective practice.
- Opportunities for collaboration and knowledge sharing.

ARMS is well positioned to assist in this area. Through its professional development programs, Special Interest Groups, conferences, communities of practice and sector networks, ARMS can play an important role in informing, training and engaging Research Management Professionals across the sector. This includes leveraging the expertise of the ARMS and Universities Australia Research Security Working Group, which is developing practical disclosure guidance informed by the experiences of university research offices, grants teams and research governance professionals. The Working Group provides an example of how sector-led approaches can support consistent implementation while remaining adaptable to future changes in funding requirements and government policy. Representatives from both universities and research institute networks, including INFIN, are contributing practical operational perspectives to this work.

The partnership between ARMS and Universities Australia in establishing the Research Security Working Group demonstrates the value of sector-wide collaboration. The Working Group provides an example of how government, institutional leaders and research management professionals can work together to develop practical solutions that support both compliance and capability building.

Recommendation

Before progressing any amendments to the Threshold Standards, Government should assess whether a material assurance gap exists that is not adequately addressed through existing or emerging legislative, funding, regulatory and institutional arrangements. This assessment should consider

whether improved coordination, clearer guidance, alignment of existing frameworks and targeted capability building would address the identified concerns more effectively than additional regulation.

If, following that assessment, Government determines that an amendment is necessary, any new expectations should be principles-based, proportionate and risk-informed. Implementation should be supported through sector-wide guidance, training, shared resources and ongoing engagement rather than relying solely on additional compliance requirements. Government should leverage existing sector capability, including ARMS and its research security networks, to support implementation and build sustainable research security capability across the sector.

Conclusion

ARMS supports the objective of strengthening Australia's research security but considers that Government should first assess whether a material assurance gap exists that is not adequately addressed through existing and emerging legislative, funding, regulatory and institutional arrangements. The existence of research security risk does not, by itself, establish that an additional enforceable Threshold Standard is necessary or would produce better security outcomes.

Experience across the sector demonstrates that the greatest implementation challenge is often not a willingness to comply, but uncertainty regarding what information must be disclosed, how requirements should be interpreted and how obligations interact across multiple regulatory frameworks. Recent experience with ARC research security disclosure requirements has highlighted the need for clear, practical and nationally consistent guidance that can be applied prospectively by researchers and institutions. Government should therefore assess whether the principal gaps relate to institutional assurance or, instead, to fragmented national guidance, inconsistent terminology, overlapping requirements and unclear responsibilities across agencies and funding bodies.

The immediate priority should therefore be to map existing obligations, align relevant frameworks and terminology, clarify the respective responsibilities of government and institutions, and establish authoritative advice and escalation pathways. This should be complemented by strengthening institutional capability, consistency and awareness through guidance, training, worked examples, shared resources and collaborative sector approaches rather than creating additional compliance burdens.

Research Management Professionals are central to the successful implementation of research security requirements. They work directly with researchers, institutional leaders, funding agencies and government to support due diligence, disclosure, governance and risk management activities. Their operational expertise can assist Government to assess whether proposed requirements are clear, workable and capable of producing consistent, reliable and decision-useful information. As such, they form a critical component of Australia's research security capability.

ARMS highlights the value of sector-wide collaboration in assessing and addressing research security risks. The Research Security Working Group established by ARMS and Universities Australia has brought together representatives from universities to develop practical solutions to disclosure and assurance challenges. This work demonstrates how government, institutions and Research Management Professionals can work together to improve consistency, strengthen capability and

support effective implementation of research security measures across the sector. ARMS is well placed to continue supporting this work through its professional development programs, Special Interest Groups, communities of practice and extensive research management networks across Australia, New Zealand and Singapore.

We welcome the opportunity to work with HESC, government agencies, Universities Australia and the wider sector to assess whether a material assurance gap exists and, if further measures are shown to be necessary, to support implementation, capability building and the dissemination of future guidance.

Key Contacts For Further Information:

Hannah Allan, ARMS President – email ARMSPresident@researchmanagement.org.au
Maria Zollo, Chief Operating Officer – email ARMSCOO@researchmanagement.org.au