7 September 2026

Higher Education Standards Committee (ATEC)
GPO Box 9880
Canberra ACT 2601

Re: Higher Education Standards Committee Research Security Consultation

Dear Sir/Madam

The Australian Digital Trust Community Group (ADT CG) under the OpenID Foundation (OIDF) welcomes the opportunity to comment on the HESC research security consultation. Please see our responses to specific questions raised in the consultation document.

On a general note, the ADT CG encourages HESC to continue to focus on interoperability and leveraging existing capability where possible. OIDF standards like OpenID for Verifiable Presentation, OpenID for Verifiable Credential issuance, OpenID Connect, FAPI 2.0, OpenID Federation, Shared Signals are likely to underpin or play a growing role in securing research in Australia and other nations.

We encourage the Australian community to use the freely available open source tests for implementers to prove out their deployments meet the security, privacy, interoperability and scale properties inherent in the specifications. Should HESC establish an accreditation or conformance scheme that includes (but may not be limited to) OIDF specifications, HESC should consider leveraging the low-cost self-certification program (https://openid.net/certification/) or the future accreditation program launching in Q2 2026 (https://openid.net/oidf-announces-new-investment-to-expand-conformance-services/). Both services are available to ecosystems, with a goal of ensuring ecosystem partners can achieve their objectives.

As a global open standards body, we welcome the opportunity to support the Australian community. As per OIDF's practice of being transparent and open, we intend to share our response to this request for comments in a blog post on openid.net in the near future.

We welcome the opportunity to discuss our comments or other related matters. Contact john.scullen@aaf.edu.au regarding any follow-up to this response.

Sincerely

John Scullen
on behalf of the Australian Digital Trust Community Group co-chairs

Executive Summary

The Australian Digital Trust Community Group (ADT CG) welcomes the opportunity to respond to the HESC research security consultation. This submission encourages HESC to strengthen research security by improving identity assurance while protecting privacy through data minimisation, avoiding duplication, preserving researcher mobility and building on existing open standards and shared sector capability.

- **Address the identity assurance gap.** Current mechanisms do not provide a common national baseline for identity proofing for staff, students, contractors, visiting researchers, adjuncts and collaborators. This limits confidence in who is participating in research and whether their institutional relationship remains valid.
- **Align new expectations with existing frameworks.** HESC should develop an approach aligned with the National Identity Proofing Guidelines and recognition of trusted international identity evidence.
- **Use open standards and shared infrastructure.** OpenID standards, including OpenID Federation, OpenID for Verifiable Credentials and Presentations, FAPI 2.0 and Shared Signals, can support interoperable trust, conformance and security signalling across institutional and national boundaries. HESC should leverage existing capabilities before setting up new bodies with overlapping remits.
- **Prepare for AI-enabled research workflows.** Assurance mechanisms should preserve a clear path to accountable human researchers and distinguish institutional context, human responsibility, machine-assisted outputs and provenance.
- **Support community-based trust and persistent identifiers.** Assurance should recognise trusted relationships within research communities and incorporate persistent identifiers such as ORCID, ROR and grant identifiers to strengthen attribution, provenance, accountability and traceability.
- **Maintain proportionate, risk-based implementation.** Any amendments to the Threshold Standards should be outcomes-based, technology-neutral and supported by clear guidance and transition arrangements. Controls should enable informed risk decisions without creating unnecessary compliance burden or friction for legitimate collaboration.

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?

Current assurance mechanisms appropriately emphasise governance, risk management, cyber security, research integrity and institutional accountability. A significant gap, however, is confidence in the identity, affiliation and current status of people participating in research. Institutions cannot adequately protect research data, intellectual property or infrastructure without knowing who an individual is, their relationship to the institution, and whether that relationship remains valid.

Australia's higher education and research sector has no common national baseline for identity proofing staff, students, contractors, visiting researchers, adjuncts, affiliates and collaborators. Institutions therefore develop local commencement practices, creating inconsistent definitions, processes and evidence requirements. This limits an organisation's ability to rely on identity and affiliation information established elsewhere. Practices around offboarding are generally prompt and reliable but identity commencement remains a weak link.

The ADT CG recommends a common identity proofing baseline for Australian research organisations, aligned with the National Identity Proofing Guidelines (NIPG)[1]. It should also map to international frameworks. Through eduGAIN, research and education communities use the REFEDS Assurance Framework to express assurance consistently across national federations, with mappings to national standards such as NIST SP 800-63 in the United States. NIPG recognises both domestic and many primary identity documents from other nations and should accommodate most international research use cases.

Privacy and data minimisation must remain key principles. Identity assurance requirements should establish the required level of confidence without unnecessarily collecting or centralising identity evidence and only retaining information that is reasonably required to conduct business functions.

The baseline must recognise trusted international identity evidence. Australian research organisations routinely engage staff, students and collaborators from other jurisdictions. Requirements focused only on Australian credentials could create unnecessary barriers to legitimate collaboration.

Open standards and shared infrastructure provide a practical path to cross-border trust. OpenID Federation enables identity providers and relying parties to establish trust through open, machine-readable metadata. Existing schemes such as ConnectID and the Australian Access Federation and its international counterparts are using OpenID Federation to support access across institutional and national boundaries through the international eduGAIN federation. HESC should build on these existing collaborative infrastructures rather than create parallel arrangements.

Assurance should also recognise established trust within research communities. Existing collaborators may be able to attest to a new participant's identity and legitimate connection to a research domain or project. Initiatives such as the First Person Project[2] show how these relationships can be represented digitally through verifiable credentials, complementing rather than replacing formal identity proofing.

Persistent identifiers should form part of the same assurance ecosystem. The Australian National Persistent Identifier Strategy[3] identifies PIDs for researchers, organisations, grants, projects, samples, infrastructure and outputs. Open, globally recognised identifiers such as ORCID, ROR and Crossref grant identifiers can strengthen attribution, provenance, accountability and traceability when linked to well-governed identity and affiliation processes.

This linkage becomes more important as AI is incorporated into research workflows. Assurance mechanisms should maintain a clear path to accountable human researchers and distinguish institutional context, human responsibility, machine-assisted outputs and provenance. Together, identity proofing, affiliation assurance, community-based trust and interoperable PIDs can strengthen research security without undermining openness, mobility or international collaboration.

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?

As outlined in response to Question 1, the principal gap is the absence of a common approach to identity commencement, proofing and affiliation assurance. New expectations should be mapped against existing obligations for cyber security, foreign interference, privacy, research integrity, data management and institutional risk, and should clarify how identity assurance supports those obligations rather than introduce a separate compliance regime.

Expectations should be outcomes-based, interoperable and capable of being implemented through shared sector services, not framed in ways that require each institution to build bespoke controls. This allows organisations to select the methods and approaches that best suit their context while remaining compatible with the broader ecosystem in much the same way that open standards work. This flexibility is particularly important in a sector with significant diversity in institutional size, research intensity and technical maturity

HESC should also allow for relevant open standards to evolve. The OpenID Shared Signals Framework (SSF)[4], for example, enables cooperating systems to exchange security events and signals. Such specifications may support faster detection and coordinated responses across institutional boundaries. Any guidance should therefore define required outcomes and assurance principles while remaining technology-neutral and capable of adopting mature open standards as they emerge.

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?

Any amendments to the Threshold Standards should improve research security without creating a new compliance layer. The central implementation challenge is integrating new expectations with already complex arrangements for cyber security, foreign interference, privacy, research governance, data management and institutional risk. Requirements should address genuine gaps and complement existing mechanisms.

Open standards support proportionate, risk-based implementation by defining interoperable protocols and data models without prescribing particular products or architectures. This allows institutions to select approaches suited to their size, research profile and technical maturity while remaining compatible with the broader ecosystem. A uniform control set could impose unnecessary burdens on lower-risk activity and divert resources from areas of greater concern.

HESC should also guard against creating friction for legitimate research. International engagement, cross-institutional partnerships and researcher mobility are strengths of Australia’s research system. Poorly coordinated onboarding, inconsistent assurance requirements or repeated due diligence could delay collaboration across institutions and

jurisdictions. Controls should enable informed decisions about risk, not discourage collaboration by default.

Requirements should therefore be outcomes-based, supported by clear implementation guidance, proportionate transition arrangements and access to shared sector capabilities. Where services already exist, such as federated identity through the Australian Access Federation or security coordination through AHECS, institutions should be able to use them rather than develop parallel solutions. Success should be measured by improved capability to identify, assess and manage research security risks, not by the volume of additional compliance activity.

References

[1] Attorney-General's Department, National Identity Proofing Guidelines (Australian Government, 2025), accessed 28 August 2026, https://www.ag.gov.au/sites/default/files/2025-09/NIPG_report.pdf

[2] First Person Project, First Person Project White Paper, accessed 28 August 2026, https://www.firstperson.network/white-paper

[3] Australian Research Data Commons (ARDC), Australian National Persistent Identifier (PID) Strategy 2024, Version 1 (2024), accessed 28 August 2026, https://zenodo.org/records/10656276

[4] OpenID Foundation, Shared Signals Working Group – Specifications, accessed 3 September 2026, https://openid.net/wg/sharedsignals/specifications/