Australian Government
Department of Education

Trust & Identity and Cybersecurity – Summary

Targeted Discussion Series (September 2024)

Summary

The consultation identified several key considerations and potential investment priorities for digital research infrastructure:

Globally connected trust and identity (T&I) frameworks for research infrastructure: A national T&I framework which is aligned with the EU's Authentication and Authorisation for Research and Collaboration (AARC) Blueprint (the de facto global standard) are important for enabling authentication and authorisation for research collaboration. Building on the work of the T&I Pathfinder, further investment is needed to uplift T&I infrastructure for national research infrastructure (NRI) and support/help NRI providers and research domains to adopt and implement the framework within the context of their domain, including instruments, data, compute, research software, etc.

Culturally sensitive T&I frameworks and infrastructure: Indigenous nations have use cases which are not common e.g. secret/sacred, women's knowledge, men's knowledge, clan/community attribution, etc, which will necessitate both deep and broad consultation. Hundreds of different nations in Australia are each entitled to form their own requirements relating to trust, identity and access in line with cultural practices on keeping and passing on knowledge.

Broadening the reach of the T&I to include researchers/collaborators outside of universities: Australian researchers collaborate with researchers in government, industry and affiliated organisations e.g. hospitals, MRI's and international groups. Investment is needed to enable researchers and collaborators who don't have an "edu.au" identity to access NRI and collaborate with researchers.

Safe and secure environments for sensitive data: Researchers from a broad range of domains are struggling with sensitive data e.g. medical/clinical data, judicial data, culturally sensitive data, etc. Investment is needed to enable a partnership of organisations across compute, data, T&I and cybersecurity and possibly others to build safe and secure research environments for sensitive data.

Implement a risk-based approach to cybersecurity: Built on appropriate common-sense frameworks and standard approaches, help NRI providers and users raise the cybersecurity of NRI through skills and knowledge enhancement, communities of practice, benchmarking and partnerships that leverage the knowledge and expertise of Australasian Higher Education Cybersecurity Service (AHECS) partners, etc.

Make research software and tool T&I and cybersecurity ready: Research software plays an important role within the NRI system and should be engineered to be aware of T&I frameworks and secured from the get-go. Investment is needed to uplift the readiness of key existing research software and provide the necessary support and expertise to help programmers and research software engineers build T&I aware and secure software.

In summary, these investments would aim to deliver more seamless NRI that is nationally and globally interconnected, that enables researchers to readily collaborate more broadly with their peers, whilst enhancing the privacy and cybersecurity of the research and innovation system.

If you'd like to provide any additional comments or feedback on the above summary, you're invited to provide these views via the online NDRI Investment Plan Consultation Survey, which can be found on the department's NDRI webpage.