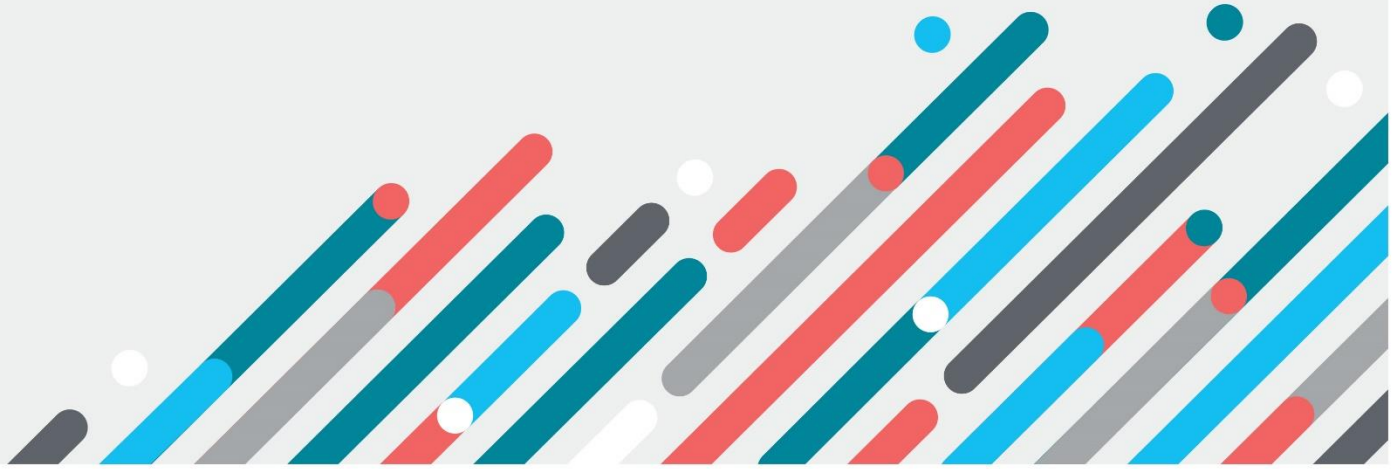
Australian Government
Department of Education

NDRI Investment Plan Consultation Survey Summary

Trust & Identity and Cybersecurity



Q28 - What measures are currently lacking or require improvement to enable Australia's researchers to conduct research in a safe and secure way, whilst protecting valuable digital resources?	**Measures lacking:** • No fully integrated trust and identity services across the NDRI landscape. Currently, the system can identify (academic and government) users, but it lacks the capability to specify which resources they can access, such as embargoed data or analytical and computing platforms • The NDRI Strategy makes no reference to personnel or physical security that would combat acts of espionage, foreign interference, intellectual property theft (either by an outsider or malicious insider) or other acts of quasi-legality (such as intellectual property theft during corporate due diligence ahead of acquisitions or mergers). • No monitoring or compliance checking on institutions that conduct sensitive or classified research in Australia as to whether they meet any current existing safeguards. • There is currently no system-wide approach to NCRIS trust and identity that aligns with government policy and international standards, to verify and assure researcher identities commensurate with the level of access assurance required. • A common entry method does not currently exist between Tier-1 high performance compute (HPC) facilities. • Lack of national trust-and-identity management and interoperability between the systems underlying it. • Many platforms lack seamless, secure authentication systems that support cross-institutional and international collaborations. • Lack of streamlined processes to implement, for example, identity management across web apps, mobile apps, special services and command line tools. • Over-reliance throughout the sector on collaboration tools supplied by commercial providers without consideration of whether the security concerns of these providers properly align with the expectations and needs of researchers. **Improvement measures:** • Comprehensive cybersecurity frameworks and risk management strategies tailored to research data and infrastructure, addressing evolving threats. • Strengthening cybersecurity measures to protect against data breaches and cyber threats. This includes advanced encryption, multi-factor authentication, and regular security audits. • Updating and enforcing data privacy regulations to ensure that sensitive research data is handled responsibly and ethically. • Cybersecurity training based on models like the NIST Cybersecurity Framework. Specialised programs would equip researchers to recognise and address evolving cyber threats.

	• Developing and standardising data management frameworks that ensure data is stored, accessed, and shared securely. This includes implementing FAIR. • Investing in secure digital infrastructure, including high-performance computing systems and cloud services, that are designed to protect sensitive data. • Partnering with cybersecurity experts and organisations to stay ahead of emerging threats and implement the latest security technologies. • Maintaining robust protection for sensitive data and resources without creating unnecessary barriers for researchers working with non-sensitive data. • Promoting ethical data practices and ensure compliance with national and international standards for data protection and privacy. • Implementing secure gateways and repositories for highly sensitive imaging data. • Creating a community of practice, across research, and industry, to enable best practice for accessing, managing and analysing sensitive data. • Persistent identifier (PID) solutions that align with the National PID Strategy are required to enable researchers and national research infrastructure (NRI) to track and report on research impact, provenance, reproducibility and return on investment. • Establishing a common protocol to enable users to have a seamless transition between Tier-1 HPC facilities. • Sensitive research data is likely to stay within the originating institution to reduce risk of it leaking unexpectedly. The NDRI should be investing in schemes to leverage this cybersecurity maturity within universities to enable research on sensitive data and still enable collaboration. • Applying appropriate PIDs on a system-wide level will improve the ability to track the impact of infrastructure and support automated access decisions across NRI (for example, PIDs). • Adapting trusted research environments like Scotland's National Safe Haven, would enable secure access to sensitive data while ensuring compliance with legal and ethical standards. Tiered security levels could balance access to high- and low-sensitivity data. • There is a growing need for trust and identity networks that inter operate and such networks are fundamental to the inclusion of Aboriginal and Torres Strait Islander people in digital infrastructure and to the concept of CARE principles. • There is a need for a national consensus on an optimised NDRI risk profile, which conveys when to trade-off between cybersecurity and open data/systems. It will ensure that any universal identity and access protocol will lead to trust and derive value from data across academia, government, and industry.

Q29 - How does Australia's future NDRI find a balance between enforcing trusted access and cybersecure measures whilst accommodating for open science principles and research with inherent risk?
 	
• Are there any international examples? Good, bad or ones which Australian researchers will have to adhere to as part of their international collaborations?
	Finding a balance:
	
	• Establishing simple, clear, and flexible agreements between institutions on a broad basis (as opposed to a per-project basis) can support appropriate, secure, and effective data sharing and transfer.
	• Developing robust data governance frameworks that ensure data is managed ethically and securely, adhering to FAIR and CARE principles.
	• Adopting appropriate risk-based approaches to governance that are evaluated on an on-going basis.
	• CARE principles require Aboriginal and Torres Strait Islander people to retain data sovereignty over their biodiversity data. This requires a complex trust and identity network both within and external to the community.
	• A tiered security approach for balancing secure access with open science, using frameworks and industry standards.
	  ○ These can support the creation of secure environments for sensitive data, while supporting open access for less sensitive research outputs.
	• Transparent governance.
	  ○ Establishing clear governance frameworks that define data sharing protocols and responsibilities.
	• Interoperability standards.
	  ○ Adopting international standards to ensure compatibility and compliance in global collaborations.
	
	International examples:
	
	• The US' National Institutes of Health (NIH).
	• The US National Security Division' Data Security.
	• Canadian National Security Guidelines for Research Partnerships.
	• Open Science Cyber Risk Profile (OSCRP) by Trusted CI that assists researchers in managing cyber risks.
	• UNESCO guidelines for Recommendation on Open Science for fair and equitable access to science and research.
	• Worldwide Large Hadron Collider Compute Grid (CERN):
	  ○ 170 computing centres in more than 40 countries, linking national and international computing grid infrastructures.
	• LifeSciences (Europe) supports pan-European life science research with multiple research organisations sharing infrastructure.
	• ACCESS (US):
	  ○ National Science Foundation (NSF) program to streamline access to national computational resources.
	• European Open Science Cloud (EOSC):

	○ balances open science and cybersecurity by a federated model to protect sensitive data, while non-sensitive data remains openly accessible. • Google Colaboratory: ○ A good enterprise example of making compute open and accessible for public research purposes in a secure manner • Globus from University of Chicago: ○ It has been used in Argonne National Laboratory (ANL), not just for national experimental facilities to reliably transfer data into the supercomputer of ANL, but it also unifies the mechanism of cyber security authentication and authorisation internationally. • Global Alliance for Genomics and Health (GA4GH): ○ It provides an example of an international model which is globally used in the Genomics Health area. • UK's Office for National Statistics Secure Research Service: ○ Provides a model where sensitive data can be accessed securely without compromising collaboration. • The UK Health Data Research Alliance operational model and case studies can be a great example for Australia, particularly the case study related to building a library for sharing tools to analyse health data.

Q30 - What are the priority NDRI investments in trust and identity, and cybersecurity that would enhance Australia's research efforts?	• Developing national trust, risk appetite and cybersecurity framework aligned with Five Safes and the Australian Cyber Strategy 2030, including its adoption in Tier-2 computing providers.
	• Implementing a robust encryption methods and multi-factor authentication to protect sensitive research data and ensure secure access.
	• Developing federated identity management systems that allow seamless and secure access to multiple resources across institutions, enhancing collaboration while maintaining security.
	• Providing comprehensive training programs to educate researchers and staff on best practices for cybersecurity, including threat detection and response.
	• Conducting regular security audits and vulnerability assessments to identify and address potential security gaps in the infrastructure.
	• Utilising AI and machine learning technologies to detect and respond to cybersecurity threats in real-time, enhancing the overall security posture.
	• Ensuring that cybersecurity measures comply with international standards and best practices, facilitating international collaborations and data sharing.
	• Investing in secure infrastructure and architectures that are interoperable across capabilities.
	• Amplifying system-wide trust and identity skills:
	  ○ Development of training and consultation programs, co-design workshops, round table events, engagement and participation with the international trust and identity community to leverage and align with best practice, technological and societal shifts.
	• Strengthening research impact tracking.
	  ○ Co-designing outcomes directly with the research infrastructure community, university research offices, the National PIDs Strategy and other partners to develop service delivery models to support and enable the use of PIDs within their systems.
	• Co-developing programs to establish the appropriate trust and identity technology systems and enabling policies to support the FAIR and CARE.
	• Investing in a coordinated model where each Australian state/territory hosts a sensitive data secure research environment would ensure shared resources, consistent standards, and better data protection.
	• Uplifting of HPC to allow for safe research of sensitive data or development of new HPC for this purpose.
	• Ageing instruments present cybersecurity risks to organisations. NDRI investments in demilitarized zone approaches will facilitate and standardise the handling of those instruments.
	• Further investment into strengthening current and emerging cybersecurity communities of practices can uplift cyber literacy for researchers and NRI operators.

	• Investing in providing Identity and Access Management (IAM) as a Service so that it is easier to integrate IAM in applications developed by the NRI providers.
	• Ensuring Australia aligns to global best practices for trust and identity. This will help provide increased longevity of current trust and identity services.
	• Federated identity management system:
	  ○ Expanding Australia's federated identifiers from healthcare to research will enable seamless access to shared resources.
	• Role-based access control:
	  ○ Australia can enhance research infrastructure by integrating automated tools to manage user access and streamline permissions, reduce administrative burden, and improve security across institutions, for safer/faster access.
	• Zero-Trust architecture model will enforcing continuous authentication and access controls, would protect sensitive research data.