

CANDIDATE INFORMATION PACK

eResearch Portfolio Manager

Includes:

- Background information on working with us
- Position description
- Abbreviated summary of the NCRIS Trust and Identity Project
- Submitting an expression of interest.





The Australian Access Federation

We are on a Mission

We're a driven group of people with a purpose to make access and authentication easier, and more cyber secure for teaching, learning and research.

AAF is an interesting company that does exciting work as a Not for Profit (NFP), which our staff and customers value.

We don't work with old tech

Who wants to work on old tech - not us! Our tech is ahead of the curve because we provide our team with the tools and empower staff to innovate. The AAF is a cloud-native company and the applications and solutions we build are at the cutting edge in identity management.

Our engineering team is conscientious about doing things right the first time, with minimal, to no 'firefighting' of existing tech. Our applications focus on identity management, authentication, and security layers. Our technical team focuses on the entire stack from Ruby on Rails code, to managing AWS infrastructure.

It's a fast-moving space and we help you, to help us:

- Interested in AWS training - sure thing, we have an annual program of training with our partner providers
- Need some time to learn some new tech - of course, our engineering team enjoy *hack time* every Friday afternoon

We do interesting end-to-end Dev/Sec/Ops work, not your standard system upgrade projects!

We are a Not-for-Profit company supporting our owners which are research and education organisations in Australia, that means we focus on delivering leading technology for our communities. AAF staff have a sense of pride and satisfaction, knowing that what we work towards helps to make the world a better place.

Did we mention we are plugged into the Australian Federal Government's eResearch infrastructure roadmap? - that's right - how many companies are part of Australia's Research tech strategy? Our staff work closely with high value innovative initiatives tackling issues from COVID, genome mapping, children's cancer research, astrophysics to identifying low wave frequencies in space and capturing gravitational waves!



We work with interesting customers and stakeholders

Just to name a few, Australia's High Performance Computing Facilities (NCI and Pawsey), Australia's national research and education network provider AARNet, leading research facilities such as the Garvan Research Institute, all the Australian Universities as well as our commonwealth science research organisation CSIRO.

We are a globally connected service working with 85 other community driven organisations who are all doing similar things around the world. This means AAF staff get to collaborate with our global community and take part in innovative activities around the globe. To demonstrate our global reach, we chair the Asia Pacific Identity Management Working Group, the working group for a globally connected authentication framework (eduGAIN) and part of the global REFEDS (Research and Educations Federations Steering Committee). We are also a member of and participate in the Australian Higher Education Cyber Security Service.

When the borders are open, AAF staff are on the road participating in initiatives and working groups with likeminded, tech professionals around the globe. In the past our staff have travelled to interesting places such as Estonia, Prague, Ireland, Norway, New Orleans, India, Iceland, Portugal and China to be part of leading-edge strategy development in trust and identity.

We are passionate about our products and services

The Federation:

The Federation is Australia's national authentication service for research and education. Using cutting edge technologies and standards the Federation delivers world-class single-sign-on that allows individuals across organisational boundaries to collaborate and access online resources within a trusted environment.

The Australian ORCID Consortium

The Australian ORCID Consortium provides a national coordinated approach to Open Research Contributor ID (ORCID – see: orcid.org). The consortium has enabled a globally unique persistent identifier for every researcher in Australia.

Consulting and Training Services

We provide bespoke consulting and support to our communities in meeting their identity and access management needs.

VerifID

VerifID, the national verification service enables universities, public agencies and commercial providers (e.g. Spotify, YouTube and Flight Centre) to accurately deliver services to Australian students and other roles in the research and education sector (see: VerifID.global).



Our company values underpin everything we do

- Innovation - an essential ingredient
- Mastery - a good mix of enthusiasm, quality, care and experience
- Trust - strengthened through our actions
- Community - achieving more together.

We pride ourselves on having a hybrid work environment

Everyone is talking about remote work these days, but the AAF was doing this long before COVID. We have been operating in a hybrid mode for over 10 years. We believe hybrid work provides flexibility and brings out the best in our staff to deliver great outcomes. Hybrid meaning, we empower our staff to work from home, and also join us in the office a couple of days a week to be part of a team that are working towards common goals. We are an innovative tech company after all, and how else do you innovate, share knowledge and professionally grow your career without spending time with your colleagues over a cup of coffee (or a beer or two).. It also gives our staff an opportunity to shine and get the promotion that they are after, rather than hiding behind a camera in a Zoom or Teams meeting. A hybrid approach is in-line with many leading tech companies and this balance supports better well being of our staff, inter-team collegiality and a more positive culture where we can do anything no matter how challenging the task may be.

AAF HQ is in the Brisbane CBD where our office is configured with hot desks and meeting rooms specifically supporting our hybrid strategy. We also have a satellite office in Perth with one of our partner organisations. We support staff in other states and territories and bring them to our office to do a comprehensive session with the team when needed.

So apart from working for an awesome NFP tech company who are doing great things, why else should you be part of the AAF?

- A 35-hour working week
- The option to salary sacrifice rent/mortgage payments (yep! that's right)
- Extra-long service leave
- 3 days bonus 'recharge leave' over the Xmas and New Year period

... and most importantly let's not forget that the AAF team prides itself on its inclusive, innovative and flexible culture that rewards and recognises great work.

If you are looking to move into a new role where you have control over what you produce, where you can make a difference and are empowered to utilise best practice techniques to create a positive global impact - then you are the person we've been looking for!



eResearch Portfolio Manager

June 2022

Position Title	eResearch Portfolio Manager
Closes	TBC
Salary Range	Dependent on qualifications and experience
Term	Fixed term, 2 years with the opportunity to extend
Location	Brisbane, although candidates from any location on the east coast of Australia who have easy access to a major airport and can work remotely will be considered
Open to	This position is open to Australian citizens and residents who have approval to work in Australia

About Us

The Australian Access Federation Limited (AAF) operates the national authentication service for Australian higher education and research organisations, enabling cross-organisational access for over 1.5 million users. Clients of the AAF's services include all Australian Universities and several prominent research organisations including the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and leading medical research institutes.

The AAF was founded in 2008 and is headquartered in the Brisbane CBD. Our applications and solutions are state of the art and cutting edge. With a strong reputation and extensive track record, AAF offers a unique opportunity to work in an innovative and progressive company recognised as a global leader in its field.

For further information about the AAF please visit <https://aaf.edu.au/about/>.

Job Description

You will be working in a dynamic environment to manage the AAF's eResearch Portfolio of programs and projects. The role will have direct responsibility for project managing all aspects of the National Collaborative Research Infrastructure Strategy (NCRIS) Trust and Identity Project. This will include aligning projects with goals, construct detailed work plans, manage teams, achieve milestones, and communicate the result across a stakeholder audience, allowing them access to trust and identity skills to integrate and implement innovative tools and modules that enables them to adopt the Trust and Identity framework for a more connected and secure NCRIS system.

Key activities include adapting existing international research system frameworks for Trust and Identity to develop a new Trust and Identity Framework for NCRIS and Australia. The role will also manage a program of approximately 8 incubator projects which will be run in partnership with various NCRIS capabilities.

You will liaise with and foster strong and enduring relations with a broad range of research communities and research infrastructure providers across the NCRIS system, universities and industry.

The role will work to the Head of eResearch and be part of a small national team of specialists, including business/eResearch analysts, identity management specialists, engineers, marketing and communications professionals.

Qualifications

The appointee will have:

- qualifications in a relevant area or extensive relevant experience; or
- extensive portfolio, program or project management experience, or
- an equivalent, alternate combination of relevant knowledge, training and/or experience.

Selection Criteria

Essential

1. Demonstrated ability to manage a portfolio of programs and projects across multiple stakeholders and organisations.
2. Demonstrated ability to successfully project manage and coordinate a range of complex projects across multiple stakeholders/organisations.
3. A strong knowledge of or experience in digital research infrastructure or similar in a higher education or research context and a proven ability to deliver project outcomes in this environment.
4. A strong track record of developing good working relationships with a broad range of stakeholders from technical specialists to senior leaders.
5. Excellent interpersonal and communication skills (verbal and written), including the ability to communicate with senior management, advisory groups, IT professionals and researchers

with extensive experience in the preparation of clear and concise documentation for varied audiences.

6. Strong financial literacy and proven experience in the successful management of budgets across a portfolio of projects.
7. A proven record of customer focus, particularly in establishing credibility and delivering against commitments.
8. Ability to work effectively with minimal direction and supervision as well as to independently act on behalf of an organisation.
9. Understanding of research and development processes, particularly as related to national digital research infrastructure.
10. Demonstrated understanding of research infrastructure challenges in both domestic and international settings.

Reporting Relationships

The position reports to the Head of eResearch, who provides broad high-level supervision. The position will be a member of the AAF eResearch Team.

Key Result Areas and Accountabilities

1. Effectively manage a portfolio of eResearch programs and projects for the AAF, including:
 - a. the development of a Trust and Identity Framework for NCRIS;
 - b. supporting the operations of the NCRIS Trust and Identity Advisory Committee; and
 - c. the implementation of incubator projects in partnership with various NCRIS capabilities.
2. Acquiring a deep understanding of the NCRIS and broader research system.
3. Act as a constructive and innovative member of the project team.
4. Demonstrate high levels of customer satisfaction in providing customer-focussed support to subscribers and AAF business units.
5. Work independently with initiative and a degree of autonomy, given broad direction.
6. Demonstrate energy and creativity in all job aspects, in particular through an efficient and quality focussed commitment to work practice.
7. Apply, develop and extend job-specific, professional and organisational knowledge to strive for professional growth and excellence in performance.
8. Create and maintain effective working relationships with all AAF subscribers, the NCRIS community and the broader research community, demonstrating exemplary professionalism at all times.
9. Openly demonstrate values of trust, integrity, honesty, fairness, and reliability, conveying a strong work ethic and a clear commitment to a harmonious work environment.
10. Ensure compliance with all relevant financial and legal requirements as applicable.
11. Adhere to the principles applicable to a "Position of Trust", and ensure that information and data is protected through compliance with all relevant and appropriate instructions, legislation, policies, and procedures.

12. Maintain a professional appearance at all times.
13. Work and act safely and take all reasonable care to protect personal health and safety and the health and safety of others.

Other Information

1. The AAF is committed to ensuring a healthy work-life balance for all staff.
2. The position is a full-time position, with normal office hours from Monday through Friday.
3. Some out of hours work may be required from time to time.
4. Travel will be required for interstate trips within Australia from time to time.
5. Applicants are required to be eligible to work in Australia.

National Research Infrastructure Gap Identification

Pathfinder for a Trust & Identity Framework & Infrastructure

Gap identified:

The 2021 National Research Infrastructure Roadmap Exposure Draft (Roadmap) recognised trust and identity (T&I) as an important part of the national digital research infrastructure (Chapter 5.8). The Roadmap also identified that it forms part of cutting edge national digital research infrastructure (Chapter 6.1).

The Roadmap noted that an investment in T&I “... would result in more secure research infrastructure and allow secure access and global connectivity for Australian researchers. Investment would provide the capacity to develop cutting edge trust and identity solutions to prepare for future cybersecurity risks and technology disruptors.”.

In 2020, the Australian Access Federation (AAF) documented this gap in its *Making the Case*¹ briefing paper along with a clear strategy on how to address it. This paper was recognised by many members of NCRIS as an accurate reflection of a clear gap within the NCRIS system. To address this gap some NCRIS projects have recognised the urgency and importance of T&I and have their own initiatives underway. These initiatives are looking at solutions that could then be implemented for the broader NCRIS system as part of a larger T&I solution.

T&I is not unique to NCRIS. The Australian Federal Government has implemented a number of digital identity initiatives over the years, including myGov, myGovID and more recently the Trusted Digital Identity Framework (TDIF). The government has also recognised the increasing threat posed to critical infrastructure² and individuals in the 2020 Cyber Security Strategy.³ NCRIS is a significant investment in infrastructure and T&I aligns closely with these initiatives. Finally, the University Foreign Interference Taskforce (UFIT) aims to provide better protection for universities.

TDIF, the Australian Cyber Security Strategy and UFIT all rely on T&I frameworks, policies and infrastructure to be effective. Not addressing T&I within NCRIS undermines these national initiatives, as well as puts Australia’s research infrastructure and individual researchers at risk. Cyber-attacks increasingly focus on exploiting weaknesses in individuals and their credentials rather than the traditional exploitation of systems. Foreign interference often starts with an individual being approached via a trusted network or relationship. A robust T&I for NCRIS would provide a higher degree of protection for researchers.

A gap in T&I within NCRIS also has consequences, including:

- Diminishing the utility, efficiency and performance of the NCRIS system;
- Australian researchers are disadvantaged in their ability to collaborate nationally and internationally, making it harder for them to access and be part of international research;
- Puts Australia at the back of the pack in the global research infrastructure space, with many other countries already moving to address T&I for their research system.

The NCRIS system is at a critical point in its evolution, with the potential for the sum of the parts of the system to far exceed the sum of the individual projects. This will require a greater level of integration between different research infrastructures and addressing the T&I gap will be a significant enabler.

If the T&I gap is not urgently addressed now in a system-wide encompassing approach, Australia risks having fragmented T&I across the research system, leading to infrastructure that is accessed by bespoke T&I islands that do not work with national and international research infrastructure. Trying to recover from a fragmented T&I landscape will be costly and take time and significant resources.

Over the next two years, the ARDC is focussing on delivering a suite of Thematic Research Data Commons (RDCs) to provide an integrated set of digital research services that can be refined and tailored as needed for a particular

¹ Making the Case, an NCRIS Trust and Identity Capability, making a more interconnected, efficient and secure NCRIS system: ncris.aaf.edu.au

² Security Legislation Amendment (Critical Infrastructure) Bill 2020: <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>

³ The 2020 Cyber Security Strategy, aims to strengthen the protection of Australians, business and critical infrastructure from sophisticated threats: <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy>

National Research Infrastructure Gap Identification

Pathfinder for a Trust & Identity Framework & Infrastructure

research community. Strategically selecting thematic areas in which to build larger, coordinated and optimised initiatives will enable the ARDC to meet the needs of the greatest number of researchers. As the ARDC moves to the Thematic RDC model, T&I is integral for ensuring researchers from academia, the public sector and industry have a seamless and cyber secure experience accessing digital research infrastructure.

Given the ubiquity of national digital research infrastructure that underpins modern research across nations and around the world, T&I impacts all Australian research communities and fields. T&I is an integral part of a researcher's daily workflow, touching every part of the research endeavour.

Solution proposed - A pathfinder for a trust and identity framework and infrastructure

The proposed solution includes an accelerator and an incubator as detailed below.

The **Accelerator** consists of the following elements:

1. A T&I Framework for NCRIS - Adapt the pre-existing work of the European Union Blueprint Architecture framework and other world-leading initiatives, to build a Trust and Identity Framework that is fit for purpose for the Australian research system, whilst ensuring that it both aligns and integrates with international frameworks and systems.

Benefits: A standardised framework to guide the development and implementation of T&I for the NCRIS system by research infrastructure providers that aligns with the Australian government TDIF and international frameworks.

Alignment: This directly aligns with the urgent needs of the ARDC Thematic Research Data Commons and BPA's BioCommons for a national approach for trust and identity for our infrastructures. Implementing an NCRIS system-wide approach would have significant positive flow on effects, providing other research infrastructure providers with reusable reference architectures that they can adopt for their own context.

Indicators/KPIs: The development of a T&I framework for NCRIS

2. Trust and Identity Cybersecurity - Deliver trust and identity infrastructure that has met a rigorous plan of cyber security. This will lower the risk of cybersecurity breaches for NCRIS and align with national and international best practice.

Benefits: A safer and more secure NCRIS environment that can be maintained and sustained at the forefront of best practice.

Alignment: This directly aligns with the Australian government's desire to protect individuals and critical infrastructure through the Cyber Security Strategy and UFIT.

Indicators/KPIs: Cyber secure T&I infrastructure.

3. Skills and Expertise - A cohort of identity and access management specialists that can work with individual research groups and research infrastructure providers.

Benefits: Provide NCRIS capabilities with the expertise they need to design, implement and manage identity and access systems that are best practice and aligned with national and international research infrastructure.

Alignment: This aligns with the need to fill the gap in the sector for skilled identity and access management specialists, the DDeRP skills working group and ARDC's skilled workforce program.

Indicators/KPIs: Increased awareness of the critical nature of T&I within NCRIS.

4. Reusable Tools and Modules - A suite of reusable T&I software solutions, tools and modules that could be used by research groups and infrastructure providers.

Benefits: Significant time savings for all NCRIS projects, standardisation across the system, with the latest tools and modules that comply with the trust and identity framework and are tested and hardened to ensure that they are as resilient as possible to cyber-attacks.

Alignment: This aligns with the ARDC's skilled workforce program.

Indicators/KPIs: Savings across the NCRIS system through adoption of reusable T&I tools and modules.

5. Access and Authentication Infrastructure - Deliver additional access, authentication and authorisation infrastructure that builds on the AAF to support the unique needs of the research sector.

Benefits: Nationally and internationally aligned T&I infrastructure that is tailored to suit the needs of cutting edge research infrastructure, resulting in significant savings and efficiency for the research system.

Alignment: As an underpinning piece of infrastructure on which everything within the T&I space is built, this aspect is viewed as more foundational rather than aligned.

National Research Infrastructure Gap Identification

Pathfinder for a Trust & Identity Framework & Infrastructure

Indicators/KPIs: Successful delivery of T&I infrastructure that meets the unique and cutting edge needs of the NCRIS system.

The **incubators** will provide access to incubator resources to NCRIS capabilities (including but not limited to a subset of the ARDC's Thematic Research Data Commons and BPA's BioCommons) to analyse and map the practises; support the integration of existing tools and services with the AAF and NDRI providers; explore access methods for researchers outside the system; and assist with the adoption of technologies and practises that enhance the cybersecurity and resilience of NCRIS.

Benefits: Act as a catalyst to fast track the adoption of trust and identity and inform future investment and fast track the adoption of a national T&I approach across the NCRIS system.

Alignment: This directly aligns with the urgent needs of the ARDC's Thematic Research Data Commons and BPA's BioCommons for a national approach for trust and identity for these infrastructure initiatives.

Indicators/KPIs: The successful implementation of agreed T&I solutions to enable NCRIS to work with the national T&I framework and infrastructure.

Timeline

The AAF is in a position to commence the establishment of project work within a matter of weeks. AAF is well connected with international partners it would need to engage with and has already been working with the ARDC and Bioplatforms Australia.

Risk

Risk 1 - Endorsement of T&I Framework by all NCRIS Projects - A failure to gain the endorsement of a national T&I framework for research would result in potential fragmentation of T&I, negating the benefits outlined in this proposal.

Mitigated likelihood - Not expected.

Mitigated Impact - Low.

Risk 2 - Tools and Modules developed by international partners prove to be not fit for purpose for Australia, requiring custom development of tools and modules.

Mitigated likelihood - Not expected.

Mitigated Impact - Low.

Risk 3 - Inability to recruit personnel with the necessary skills in identity and access management due to chronic labour market shortages.

Mitigated Likelihood - Expected.

Mitigated Impact - Moderate.

Risk 4 - The capacity of NCRIS projects to engage in incubators is limited, causing delays.

Mitigated Likelihood - Not Expected.

Mitigated Impact - Low.

Risk 5 - Inability to secure the necessary expertise to address cyber security.

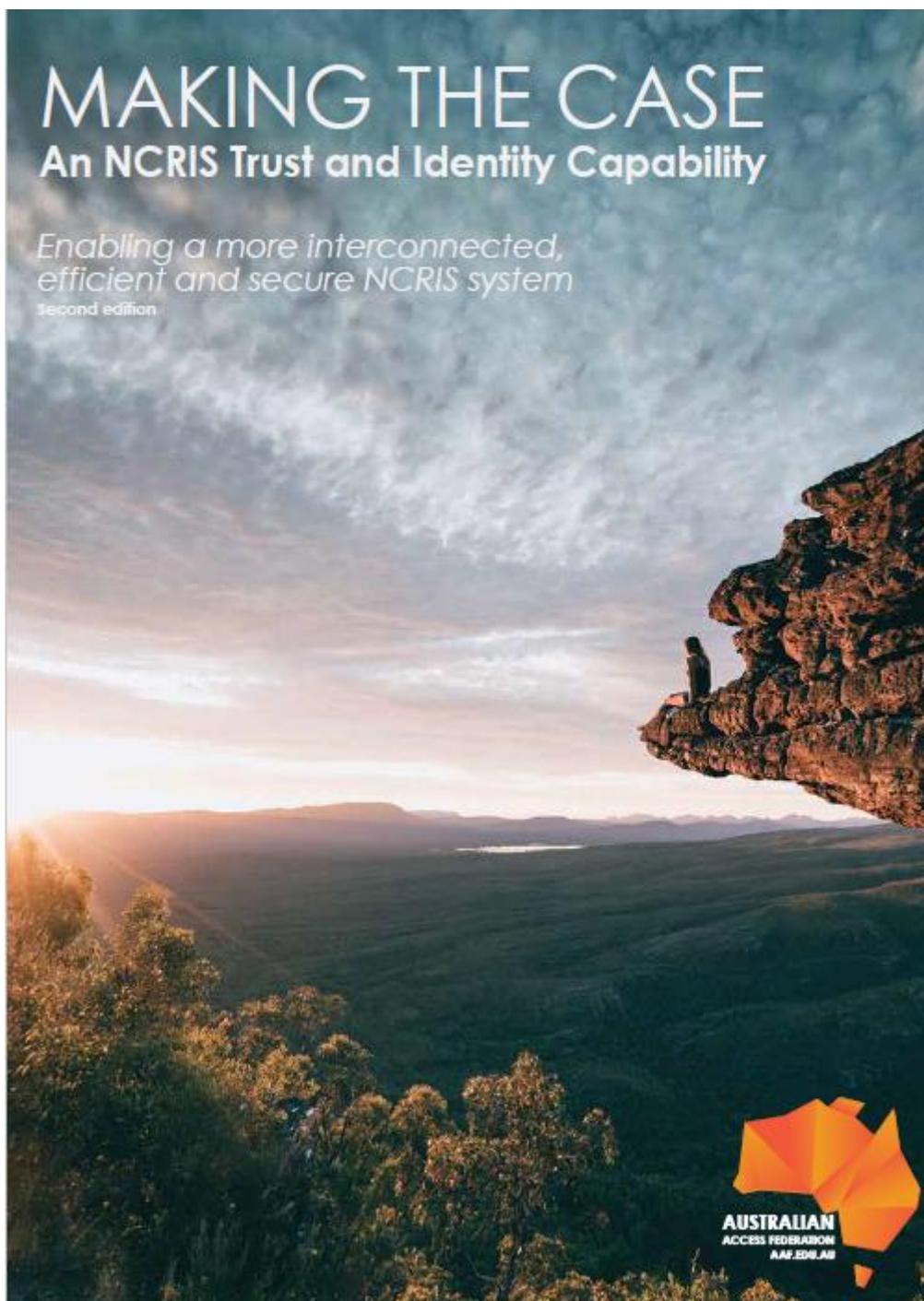
Mitigated Likelihood - Certain.

Mitigated Impact - Moderate.

Resources Required:

The proposed resources required are detailed below:

- Salaries and on costs of dedicated staff to support the pathfinder;
- One-off access to international specialist identity expertise;
- Technology platforms for research specific access and authentication infrastructure;
- Software licensing of existing solutions (2 * incubators year 1; 4 incubators year 2);
- Engagement with the NCRIS community; and
- General project overheads, including limited travel, governance, contract management and other office and project overheads.



Want more information on our vision for Trust and Identity in the research system?

Visit ncris.aaf.edu.au



Expressions of interest and/or questions
should be directed to: Sarah Nisbet

e: sarah.nisbet@aaf.edu.au