Australian Government | NIC National Intelligence Community

National Intelligence Explore Award
Research Topics 2026-27

Reference	Topic Title
NIEA-2027-001	RISCV exploitation techniques and state of the market
NIEA-2027-002	Translating epidemiological-based violence prevention approaches to enhance threat identification and disruption in countering violent extremism
NIEA-2027-003	Multi-source intelligence fusion and decision advantage
NIEA-2027-004	AI-enabled psychological inference for personnel security
NIEA-2027-005	Insider risk in the Australian context
NIEA-2027-006	The intersection between immigration, diaspora exploitation, and serious organised crime in Australia
NIEA-2027-007	Opportunities for serious organised crime in Australia's increasing reliance on emerging technologies and the Internet of Things
NIEA-2027-008	Integration of artificial intelligence into intelligence workflows
NIEA-2027-009	Scalable entity resolution using quantum computing
NIEA-2027-010	Engineering biology for sustainable power generation
NIEA-2027-011	Advancing risk assessment capabilities and understanding of LLMs and biological design tools

NIEA-2027-001

Unclassified Research Topic Title:
RISCV exploitation techniques and state of the market

Unclassified Key Words:
RISCV, Exploitation, Instruction Set Architecture, Exploit Mitigation, Internet of Things.

Unclassified Research Topic Description, including Problem Statement:
RISCV is an emerging open-source, extendible Instruction Set Architecture (ISA) which appears to be growing in popularity in the Internet of Things (IoT) space as it is royalty free. Due to it being a relative newcomer there is a lot less open-source information/resources on exploitation in comparison to other ISAs such as ARM or x86. We invite applications for research that reviews exploitation efforts/research against RISCV and undertakes novel research into exploitation techniques to ensure that the National Intelligence Community (NIC) has knowledge of RISCV exploitation at parity with existing ISAs such as ARM and x86.

Unclassified Example Approaches:
Literature review of existing approaches to RISCV exploitation as well as an analysis of the state of the market and RISCV adoption. We are also interested in details of where vendors have extended/modified the instruction set, especially security-focused extensions.

Proof of concept exploits (including defeats for common exploit mitigations such as stack canaries, data execution prevention (DEP), Address Space Layout Randomisation (ASLR)) either against real RISCV powered devices, or emulated environments.

Unclassified Relevance to the Intelligence Community:
IoT represents a growing capability for society but with increased utility comes potential threats, which are of interest to the NIC. It is prudent to stay informed of research and market trends in this field.

References:

- Harris *et al*. (2021). Morpheus II: A RISC-V Security Extension for Protecting Vulnerable Software and Hardware. DOI:10.1109/HOST49136.2021.9702275
- Buckwell *et al.* (2024). Execution at RISC: Stealth JOP Attacks on RISC-V Applications. https://doi.org/10.1007/978-3-031-54129-2_22
- Brohet *et al*. (2023). A Survey on Thwarting Memory Corruption in RISC-V. https://doi.org/10.1145/3604906
- Shivakumar and Heng (2025). Sustaining Standards Leadership: The United States Cannot Disengage from RISC-V.

When preparing proposals please be duly respectful of:
- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-002

Unclassified Research Topic Title:
Translating epidemiological-based violence prevention approaches to enhance threat identification and disruption in countering violent extremism

Unclassified Key Words:
CVE, disruption, diversion, early-intervention, epidemiology, public health, transmission vector

Unclassified Research Topic Description, including Problem Statement:
Researchers have been using transmissible disease paradigms to build responses to violence since the 1980s. In this model, violence is conceptualised as a pathogen which can be transmitted by contact with a carrier. This analogy translates easily to the notion of radicalisation, both in support of a violent ideology (cognitive radicalisation) and the acquisition of capability or mobilisation to violence (behavioural radicalisation). The value in this approach is to identify transmission vectors for radicalization and develop ways that offer the greatest chance of disrupting the transmission of violent intent or capability through a digital or in-person network.

Unclassified Example Approaches:
An interdisciplinary structure combining ethnographic research in 'at-risk' communities and a digital humanities approach to online engagement informing agent based or statistical modeling to formulate a susceptible-exposed-infected model. A diversity of data sources and qualitative interpretation of the resulting model should be embedded in the process to counter potential bias effects.

Unclassified Relevance to the Intelligence Community:
The intelligence community would benefit from adding a 'susceptible-exposed-infected' vector transmission approach to support Countering violent extremism (CVE) policy formulation, particularly in the areas of community resilience and support for targeted interventions. Further, access to this modelling may be used alongside existing analytical techniques to inform operational awareness of the emergence of new threat vectors and tactical decisions on modes of disruption.

References:

- DeGue, S., Liu, G. S., Frederique, N., Le, V. D., & Simon, T. R. (2026). Applying the public health approach to prevent targeted violence in the United States. Psychology of violence, 16(2).
- D'Inverno, A. S., & Bartholow, B. N. (2021). Engaging communities in youth violence prevention: Introduction and contents. American journal of public health, 111(S1), S10-S16.
- Gobaud, A. N., Jacobowitz, A. L., Mehranbod, C. A., Sprague, N. L., Branas, C. C., & Morrison, C. N. (2022). Place-based interventions and the epidemiology of violence prevention. Current epidemiology reports, 9(4), 316-325.
- Grissom, S. O. (2022). Public Health Approach to Countering Violent Extremism and Proposing the Chain of Violent Radicalization. Handbook of Security Science, 977-1000.
- Keyes, K., Tracy, M., & Cerdá, M. (2018). Reducing Urban Violence: A Contrast of Public Health and Criminal Justice Approaches. Epidemiology, 29(1), 142–150.

When preparing proposals please be duly respectful of:
- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and

- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-003

Unclassified Research Topic Title:
Multi-source intelligence fusion and decision advantage

Unclassified Key Words:
multi-source intelligence fusion; decision advantage; AI-assisted analysis; advanced analytics; entity resolution; identity intelligence; attribution; synthetic content detection; cyber security analytics; situational awareness; secure collaboration; knowledge management; human-technology integration; intelligence-led decision making

Unclassified Research Topic Description, including Problem Statement:
Modern intelligence and national security environments are characterised by rapidly expanding data volumes, increasingly sophisticated adversaries, fragmented information sources and accelerating decision-making requirements. Intelligence agencies must identify, collect, analyse and operationalise information from people, networks, transactions, sensors, communications, cyber environments and emerging technologies to produce timely and actionable intelligence. Current approaches often struggle to fuse large, disparate, incomplete and rapidly changing structured and unstructured datasets into coherent intelligence products at the speed required by modern operations. The research problem is to develop a trusted, sovereign capability for advanced multi-source intelligence fusion, secure collaboration, automated analysis and decision support across law enforcement, intelligence and national security domains.

Unclassified Example Approaches:
Research could investigate advanced information fusion methods to automatically identify, combine and contextualise intelligence from disparate sources; entity resolution and attribution techniques to improve understanding of identities, behaviours, networks and adversarial tradecraft; AI and machine learning techniques for intelligence discovery, triage and prioritisation; cyber and security analytics for detecting emerging threats, infrastructure vulnerabilities and insider risks; collaborative situational awareness and decision-support workflows for complex operational environments; and human-technology integration approaches that maintain transparency, governance, legal compliance and human oversight. Activities could include prototyping integrated analytic workflows, evaluating automation against sparse or incomplete datasets, developing trusted knowledge-management architectures, and validating decision-support approaches against operationally realistic intelligence scenarios.

Unclassified Relevance to the Intelligence Community:
The topic aligns directly with National Intelligence Community priority challenge areas including covert collection, identity management, emerging data science, cyber security, situational awareness, social behavioural analysis and socio-technical systems. Successful research would improve the ability to identify patterns, relationships, risks and opportunities across diverse intelligence sources; enhance collaboration and intelligence sharing between agencies and operational partners; improve detection of emerging threats, influence activities and adversarial behaviours; and accelerate the production of actionable intelligence and operational assessments. It would also support sovereign intellectual property in advanced intelligence fusion technologies and establish national capability in multi-source intelligence analysis and decision support.

References:

- The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis
- AI-The-Future-of-Intelligence-Analysis-SCSP-ASPI-Report.pdf
- Intelligence-led policing | Australian Institute of Criminology

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-004

Unclassified Research Topic Title:
AI-Enabled Psychological Inference for Personnel Security: Detecting Risk-Relevant Characteristics and Temporal Change to Augment Professional Assessment

Unclassified Key Words:
Artificial intelligence; machine learning; natural language processing; psycholinguistic analytics; personnel security; psychological assessment; continuous evaluation; insider risk; human-AI teaming

Unclassified Research Topic Description, including Problem Statement:
Australia's national security depends on the trustworthiness of individuals granted access to its most sensitive information, facilities, and capabilities. Psychological assessment is a cornerstone of the personnel security framework; it identifies characteristics that may indicate vulnerability to coercion, exploitation, or untrustworthy behaviour. The NIC faces growing demands on its capacity to effectively assess and maintain security clearances as the community grows and becomes more diverse.

Emerging advances in artificial intelligence (AI), machine learning, and psycholinguistic analytics offer an opportunity to reimagine this process—not by replacing professional judgement, but by augmenting it. AI systems that can analyse behavioural and linguistic data to infer psychological characteristics, and critically, detect meaningful changes and predict trajectory in those characteristics over time, could serve as a force multiplier for professionals. Such tools could identify and prioritise cases for expert review, flag emerging concerns between scheduled assessments, and provide interpretable evidence to support clinical decision-making.

While AI has been applied to discrete psychological inference tasks in clinical and commercial domains, its application to personnel security remains underexplored. Key unanswered questions include:

- Can AI reliably infer psychological characteristics relevant to security risk from behavioural and linguistic data, in addition to personality traits?
- Can AI detect meaningful temporal change in these characteristics, distinguishing normal variation from shifts warranting attention and/or intervention?
- How can AI outputs be made interpretable, explainable, and actionable for clinical professionals?
- What governance frameworks are required to ensure such systems operate lawfully, ethically, and without bias?

Unclassified Example Approaches:
Research could examine the validity, reliability, interpretability, and operational feasibility of AI approaches for the purposes identified above. Potential data sources include information already collected through existing processes, as well as other authorised digital sources where lawful and proportionate. Ethical considerations—privacy, consent, transparency, algorithmic bias, and governance—must be central to the research design.

The NIC seeks evidence on what works, what doesn't, and under what conditions. We are particularly interested in interdisciplinary approaches that bridge computer science, psychology, and security studies.

Research could involve:

- Systematic review and meta-analysis of machine learning, NLP, and psycholinguistic approaches for inferring psychological characteristics from behavioural and linguistic data, including temporal change detection for personnel security applications.
- Feasibility assessment and prototype development using simulated or de-identified data to evaluate AI-enabled psychological inference.
- Comparative evaluation of commercial AI tools and custom models for personnel security workflows.
- Governance and ethics framework development addressing the legal, ethical, and operational requirements for deploying AI in high-stakes personnel security decisions.

Unclassified Relevance to the Intelligence Community:
This research addresses a shared challenge across the Five Eyes (FVEY) intelligence community: how to maintain rigorous personnel security assessment at scale, without compromising the professional judgement that underpins clearance decisions.

By investigating AI that augments rather than replaces psychologists, this work has the potential to:

- Improve the efficiency and responsiveness of personnel security processes.
- Strengthen the evidence base for clearance decisions.
- Enable more proactive identification of personnel security concerns.
- Ensure human oversight remains central to all assessment and adjudication.
- Establish governance frameworks that maintain public trust and legal compliance.

The research will generate actionable insights for NIC agencies and FVEY partners grappling with similar workforce and capability constraints. Findings will inform procurement decisions, capability development, and policy settings for AI-enabled personnel security tools.

References:

- Lenzenweger, M. F., & Shaw, E. D. (2022). The critical pathway to insider risk model: Brief overview and future directions. Counter-Insider Threat Research and Practice, 1(1).
- Baweja, J., Barr, J., & Murphy, C. (2025). *Responsible Artificial Intelligence (AI) for Insider Threat* (Report No. PNNL-38436). Pacific Northwest National Laboratory.
- Wilder, U. M. (2017). Why spy? The psychology of espionage. Studies in Intelligence, 61(2), 19–36.

When preparing proposals please be duly respectful of:
- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-005

Unclassified Research Topic Title:
Insider risk in the Australian Context: identifying unique indicators of insider risk in Australia and considering their implementation in identifying and managing insider risk.

Unclassified Key Words:
Insider threat; indicators; management strategies; critical pathway to insider risk

Unclassified Research Topic Description, including Problem Statement:
While there is a substantial body of research on insider risk, most studies and case examples originate from the United States and United Kingdom. As liberal democracies and trusted partners, the insights derived from this research have been instrumental in shaping Australian insider threat concept and management frameworks. However, there remains a significant gap in the literature regarding the Australian experience of insider risk and threat management. Given Australia's distinct cultural, social and organisational context, this study seeks to determine whether there is a uniquely Australian experience of insider risk and to gauge the effectiveness of current threat management approaches. The findings will inform future policy development and support the creation of training and reference materials for Australian insider threat specialists, vetting analysts and psychologists.

What does insider risk look like in Australia?

- Are there indicators of insider risk that are specific to the Australian context?
- Are there universal indicators that are relevant across different cultures/countries?
- Do indicators of insider risk (both universal and Australian) change based employment type (i.e. government, non-government, multi-national corporations, small business)?
- What impact/lack of impact does non-western/western culture have on the relevance and applicability of current insider risk indicators? How should cultural factors be considered in the identification and management of insider risk in Australia?

How are Australian insider risks managed?

- Are there unique mitigators of insider risk in Australia?
- Are specific types of management stratiges more effective than others? If so what are they?
- What are the social and/or cultural impacts of problematic organisational responses in Australia?

Extrapolating the Critical Pathway to Insider Risk (CPIR) in Australia

- The CPIR suggests that individuals demonstrating certain personal predispositions are more likely to undertake an insider act and/or demonstrate concerning behaviours in response to stressors. However, there are gaps in the literature regarding individuals who demonstrate and experience the requsite predispositions, stressors and behaviours but do not commit an insider act.
- Are there specific indicators, or groups/combinations of indicators, for individuals who progresses down the CPIR but are un- or less likely to undertake and insider act? If so, what are they?

Unclassified Example Approaches:
A literature review could examine the existing research on insider risk and threat management, focusing on US, UK and Australian literature to consider the extent to which these findings and frameworks apply to the Australian context.

Analysis of Australian insider threat case studies could examine how insider risks manifest within Australian organisational, cultural and security contexts, and may identify any common indicators, themes, drivers or risk factors that differ from international examples. Considering a broad range of insider threat cases including espionage, unauthorised disclosure, fraud, sabotage and other forms of insider misconduct could offer insights relating to the diversity and distinctiveness of Australian human, cultural and organisational risk factors. And could identify opportunities to assess and mange uniquely Australian indicators relevant to insider risk and threat management.

The research may involve interviews with government and industry personnel security and insider threat practitioners, such as vetting analysts, psychologists and insider threat specialists. This approach could provide valuable insights into how insider risk is identified, assessed and managed within Australian organisations, and whether practitioners encounter indicators that differ from those reflected in US and UK research. The inclusion of practitioner perspectives may enable a nuanced comparison between academic literature and operational practice in Australia.

Unclassified Relevance to the Intelligence Community:
There is significant work underway to strengthen insider threat programs across the Australian Government, including within the National Intelligence Community. Effective insider threat programs, informed by contemporary research and best practice, enable organisations to proactively and proportionately identify, assess and manage insider risk. This research will support efforts led by the Office of National Intelligence to better understand and manage insider risk within Australia's unique security, organisational and cultural context.

The findings will also contribute to broader collaboration across the FVEY intelligence community by providing evidence-based insights into the Australian experience of insider risk and threat management. By identifying any distinct Australian characteristics, challenges or approaches, the research will help inform the ongoing development of policy, practitioner training, and operational frameworks designed to strengthen insider risk management capabilities across government and industry.

References:

- Application of the Critical-Path Method to Evaluate Insider Risks, Dr Eric Shaw and Laura Sellers, Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)

When preparing proposals please be duly respectful of:
- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-006

Unclassified Research Topic Title:
The intersection between immigration, diaspora exploitation, and serious organised crime in Australia

Unclassified Key Words:
Serious organised crime; SOC; migrants; Australia

Unclassified Research Topic Description, including Problem Statement:
Australia is a destination for various migrant cohorts, including temporary, first-generation and irregular (i.e. persons moving outside regular migration channels), however, the migration experience can make individuals vulnerable to exploitation by serious organised crime (SOC).

This research seeks to understand linkages between SOC and migrants and explore:

- Tactics SOC presently use to recruit, exploit, and utilise this cohort for various illegal activities as both victims and actors.
- Whether tactics are evolving and, if so, in what ways.
- The major drivers underpinning migrant vulnerability to witting or unwitting participation in illicit activities. These drivers include an individual's visa conditions, level of legal protections, and perceptions of immigration status, and
- any commonalities in demographic characteristics of migrant cohorts targeted for exploitation, broken down by illicit activity.

Unclassified Example Approaches:

- Examine through the lens of a select group of illicit activities how SOC actors currently recruit, coerce and retain migrants and – by extension – indicators of evolving methodologies, trends, and tactics used. The choice of illicit activities to include in research would be informed by current data on cohort involvement.
- Examine through the lens of a systems-level disruptor, like emerging tech and connectivity, to map out the evolving linkages between these migrant cohorts and SOC.
- Examine whether SOC recruitment patterns of migrants differ between nationalities, ethnoreligious, political or other groupings within nationalities, visa sub-classes, age, gender, pre-existing perceptions of authority, and immigration status.
- Identify opportunities for improving intelligence activities, policies, community engagement, and law enforcement strategies to reduce the risk of exploitation.

Unclassified Relevance to the Intelligence Community:
This research will enable greater understanding of the intersection between immigration, diaspora exploitation, and SOC in Australia; an area that remains underexplored in both academic literature and intelligence. As migration patterns shift and new diaspora communities emerge, it is essential to understand how criminal groups adapt their strategies to target vulnerable temporary or newly arrived populations in Australia.

The findings of this research would have significant, strategic implications for intelligence and law enforcement strategies and polices in Australia. Understanding how the vulnerabilities of migrants are exploited will, in turn, enable authorities to identify how to better harden policies and regulatory frameworks to deter SOC actors. This understanding will also inform downstream services, like victim support, and enable the development of more targeted anti-crime strategies to address the root causes of exploitation.

In addressing both the criminal opportunism and victimisation aspects, this research will contribute to a more nuanced understanding of how to safeguard vulnerable populations while combating SOC on a national and international level.

References:

- United National Office on Drugs and Crime - Research Brief on Transnational organized crime (https://www.unodc.org/documents/data-and-analysis/tocta/Brief_2026/Transnational_Organized_Crime_Brief_2026.pdf)
- The costs of serious and organised crime in Australia, 2023–24
- Rapid Review into the Exploitation of Australia's Visa System Report
- Migration system enabled worst crimes known to humanity | The Canberra Times | Canberra, ACT

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-007

Unclassified Research Topic Title:
Opportunities for serious organised crime in Australia's increasing reliance on emerging technologies and the Internet of Things

Unclassified Key Words:
Serious organised crime; SOC; internet of things; emerging technologies

Unclassified Research Topic Description, including Problem Statement:
As digital technology and connectivity through the Internet of Things (IoT) continues to evolve, Australia is navigating an increasing reliance as an end user. These developments, while beneficial in terms of enhancing convenience, productivity, and connectivity, also create new vulnerabilities that serious organised crime (SOC) groups are already seeking to exploit. From smart devices to cloud computing, and the expansion of digital financial systems, technology has become deeply embedded in how everyday Australia functions. This ubiquity and reliance are central to SOC exploitation opportunities, such as espionage, hacking, fraud, cyber extortion, data theft, illicit digital transactions and even physical sabotage. In this context, SOC groups will not only exploit existing digital vulnerabilities but also adapt their traditional crime models to take advantage of emerging technological trends.

This research topic seeks to investigate the potential growth areas for SOC in the context of Australia's digital transformation, including the alignment between emerging technological trends and SOC operational models, with a focus on the future state.

Unclassified Example Approaches:
- Examine current and evolving methodologies, trends and tactics used by SOC groups for exploiting digital vulnerabilities, including alignment between emerging technological trends and traditional and evolving criminal models.
- Identify emerging technologies (e.g., IoT, AI, blockchain, cloud computing) that present opportunities for SOC exploitation in Australia.
- Investigate the intersection of technology and SOC operations, including cyber extortion, data theft, cryptocurrency fraud, and IoT-related crime.
- Forecast future SOC trends in the technology space, including likely sectors and technologies at risk. This risk could be considered from angles beyond the technology itself, such as the regulatory environment and anticipatory capacity of government to harden the environment.
- Identify opportunities for mitigating SOC risks through improved intelligence collection, policy, regulation, and cross-sector collaboration.

Unclassified Relevance to the Intelligence Community:
This research addresses a critical and underexplored intersection between technological innovation and serious organised crime in Australia. As digital infrastructure becomes more embedded in everyday life, SOC groups are increasingly exploiting these systems to expand their operations, evade detection, and target vulnerable sectors.

By identifying current and future risks, this study will inform intelligence processes, policy development, law enforcement strategies, and cybersecurity practices. It will also support industry and government collaboration to build more secure digital environments and reduce the impact of SOC on Australia's economy and society.

Additionally, this study will contribute to the global dialogue on cybersecurity and digital

crime, offering a focused perspective on the Australian context. As such, it will be an essential resource for Australian stakeholders in shaping the future of digital security and mitigating the risks posed by SOC in an increasingly interconnected world.

References:

- Crime without borders: the digital shift | Australian Criminal Intelligence Commission
- EU-SOCTA-2025.pdf
- Technology allows organised crime to carry out hits, distribute drugs from a distance - ABC News
- Organized Crime and AI: 5 Topics We Are Monitoring in 2026
- NCA launches the National Strategic Assessment 2026 - National Crime Agency
- Is government losing the battle against tech-enabled transnational organised crime? - Government News

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-008

Unclassified Research Topic Title:
Integration of artificial intelligence into intelligence workflows

Unclassified Key Words:
Artificial Intelligence; intelligence workflows

Unclassified Research Topic Description, including Problem Statement:
Integration of Artificial Intelligence (AI) tools and processes into intelligence workflows has the potential to improve the quality, consistency and actionability of intelligence products while maintaining analytical rigour, transparency and human accountability.

The success of AI is often measured in immediate productivity gains, such as hours of analyst effort saved or improvements in compliance to standards. An additional measure for NIC agencies to consider is whether AI use is strengthening the longer-term capability and resilience of its intelligence system more holistically.

The research would examine the conditions under which AI use in NIC intelligence functions builds intelligence capability over time. This includes the capability of individual analysts, teams, agencies and the broader intelligence community. Examples of resilience could be analysts' ability to reason effectively without AI assistance, and an example of capability could be improvements in the analytical integrity and transparency of assessments where AI is used in any part of the production life-cycle, training of analysts or record-keeping.

The research would take a system-level view, considering the interaction between analyst practice, tool design, training, supervision, organisational culture, policy, governance and management. Rather than replace analytical judgement, this research seeks to examine how AI can *support* intelligence tradecraft while preserving and ideally developing the human analytical capabilities on which the intelligence system depends.

Unclassified Example Approaches:
- Examine how the use of AI-assisted analytical support influences analysts' ability to independently generate, test and challenge analytical judgement.
- Explore how AI can support structured analytical techniques, challenge, identify analytical gaps and provide coaching-like support without weakening independent analytical reasoning.
- Explore options for measuring the impact of AI on compliance with intelligence standards or process, as well as impacts on the diversity and appropriate selection of analytical approaches used in practice at an individual, team and agency level.
- Examine how intelligence analytical tasks (for example, information collation, pattern detection, hypothesis generation, assessment) can be systematically classified according to the capabilities and limitations of AI tools, and identify which task types are best-suited, appropriate or unsuitable for AI assistance.
- Examine how agencies could assess whether AI use is developing or degrading analyst capacity for independent analysis and judgement.
- Identify practical metrics for prioritising, monitoring and evaluating AI integration that move beyond short-term productivity and consider intelligence system strength and resilience.

- Consider how differences or alignment in AI capability, access and interoperability across the NIC impact opportunities for collaboration.

Unclassified Relevance to the Intelligence Community:
The proposed research would support the current activities of the intelligence community. It would provide a strong basis for evaluating AI projects and support guidance and policies that do not compromise overall intelligence capability. This would help agencies assess and manage the need for immediate productivity gains against long-term intelligence capability needs.

The findings could inform the design and implementation of AI tools, workforce development, supervision, governance and organisation policy across intelligence functions. This could include developing 'right tool for the task' framework and practical guidance for agencies to support analytical development of their staff, long-term intelligence system resilience and strategic decision on NIC collaboration.

References:

- RAND, 2025, Improving sense-making with Artificial Intelligence, https://www.rand.org/pubs/research_reports/RRA3152-1.html
- The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis, CSIS, October 9 2020, https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologies-transform-intelligence-analysis
- McMahon, 2024, Analytical Tradecraft Standards in an Age of AI, https://www.belfercenter.org/sites/default/files/2024-08/Gerald%20McMahon%20Belfer%20Report%20IntelProject_AI_AnalyticTradecraft.pdf
- Australian Strategic Policy Institute, The Future of Intelligence Analysis: U.S.-Australia Project on AI and Human Machine Teaming, September 2024, AI-The-Future-of-Intelligence-Analysis-SCSP-ASPI-Report.pdf

When preparing proposals please be duly respectful of:
- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-009

Unclassified Research Topic Title:
Scalable entity resolution using quantum computing

Unclassified Key Words:
Privacy-preserving entity resolution; quantum computing; cryptographic protocols

Unclassified Research Topic Description, including Problem Statement:
Entity Resolution (ER) at enterprise scale—linking disparate, noisy datasets across distributed databases without relying on universal unique identifiers—presents a fundamental trade-off between computational scalability, comparison accuracy, and strict data privacy. Classical state-of-the-art frameworks, such as the P-Signature approach introduced by Zhang et al. (2018), mitigate high dimensional comparisons by extracting low-frequency probabilistic subrecords for candidate blocking, followed by distributed connected-components graph algorithms to compute transitive links on parallel databases.

However, as data scales to billions of records across multi-party organizational boundaries, classical methods encounter severe scaling limits in candidate signature search spaces, fuzzy string comparison overheads, and graph partitioning complexity. Furthermore, integrating classical Privacy-Preserving Record Linkage (PPRL) protocols—such as Bloom filter encodings, Homomorphic Encryption (HE), or Secure Multi-Party Computation (SMPC)—introduces heavy performance bottlenecks that severely hinder real-time analytics.

This research investigates the integration of Quantum Computing Algorithms with Quantum Cryptographic Protocols to modernize large-scale, privacy-preserving entity resolution. By reformulating probabilistic signature generation as a quantum unstructured search and combinatorial optimization task onto quantum walk and variational optimization frameworks, this approach promises to bypass classical computational bottlenecks. Simultaneously, embedding Quantum Homomorphic Encryption (QHE) and Blind Quantum Computation (BQC) directly into the entity resolution lifecycle ensures that record similarity evaluations, signature matching, occur over encrypted quantum states without revealing sensitive quasi-identifiers or unlinked entity relationships.

The core problem addressed by this project is the lack of a unified, fault-tolerant quantum framework capable of accelerating high-precision probabilistic entity resolution while guaranteeing information-theoretic privacy across untrusted cloud environments. Existing classical PPRL frameworks remain vulnerable to graph-based re-identification attacks and cannot scale to complex multi-party fuzzy record linkages without prohibitive computational overhead. Conversely, while emerging quantum algorithms offer theoretical quadratic and exponential speedups for database search and graph optimization, they have not yet been adapted to handle noisy, real-world subrecord distributions or privacy-preserving data matching workflows. This research bridges this critical gap by developing a scalable, hybrid quantum-classical architecture that unifies probabilistic signature blocking, quantum fuzzy string matching, and secure graph transitive linkage.

Unclassified Example Approaches:
- Grover-Based Quantum Counting for Probabilistic Signature Extraction: Utilizing Quantum Counting algorithms to estimate subrecord recurrence frequencies ($k = \vert{}R_s\vert{}$) with a quadratic O(√N) speedup over classical database scans, accelerating the calculation of Poisson signature probabilities (p_s) across massive unlabelled datasets.

- QAOA-Driven Candidate Signature Selection: Formulation of candidate signature grammar extraction as a variational combinatorial optimization problem using the Quantum Approximate Optimization Algorithm (QAOA), balancing string brevity against entity distinctiveness.
- Quantum Swap-Test Kernels for Encrypted String Distance: Implementing quantum overlap and swap-test circuits to evaluate string similarity indices (such as Jaccard, edit distance, or q-gram overlap) directly in Hilbert space using O(log N) quantum state dimensions.
- Quantum Homomorphic Encryption (QHE) for Secure Feature Matching: Encrypting quasi-identifiers into encrypted quantum states $\vert{}\psi\rangle$ to allow untrusted processing units to perform probabilistic signature comparisons without decrypting sensitive underlying text.
- Quantum Walk Transitive Linkage Protocols: Adapting spatial quantum walks and span programs to evaluate s-t graph connectivity, replacing classical iterative database join-and-group operations (c(L)) for fast cluster identification.
- Sub-Problem QAOA for Ambiguous Cluster Resolution: Applying Sub-Problem Quantum Alternating Operator Ansatz (SQAOA) to resolve dense, over-linked connected components via modular correlation clustering, reducing false-positive linkages in high-noise data environments.

Unclassified Relevance to the Intelligence Community:
The proposed research would support the current activities of the intelligence community who have large scale entity resolution matching algorithms deployed and are unable to scale them cost effectively and share the results whilst maintain privacy and security.

References:

- Lee, S. et. al., (2025). Secure privacy-preserving record linkage system from re-identification attack. PLOS ONE, 20(1), e0314486. https://doi.org/10.1371/journal.pone.0314486
- Stetsikas, L. (2026). Privacy-Preserving Record Linkage: Past, Present and Yet-to-Come. In Proceedings of the 29th International Conference on Extending Database Technology (EDBT '26), 24–27 March 2026, Tampere, Finland.
- Wang, J. et. al., (2022). Cooperative and Competitive Multi-Agent Systems: From Optimization to Games. IEEE/CAA Journal of Automatica Sinica, 9(5), 763–783. https://doi.org/10.1109/JAS.2022.105506
- Zhang, Y. et. al., (2018). Scalable Entity Resolution Using Probabilistic Signatures on Parallel Databases. In Proceedings of the 27th ACM International Conference on Information and Knowledge Management (CIKM '18), 2213–2221. https://doi.org/10.1145/3269206.3272016

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-010

Unclassified Research Topic Title:
Engineering biology for sustainable power generation

Unclassified Key Words:
Power sources; batteries; energy harvesting; engineering biology; synthetic biology; microbial fuel cells; soil microbial battery; electrogenic bacteria; bio-electricity; Internet of Things; low-power devices; sustainable energy; remote sensing

Unclassified Research Topic Description, including Problem Statement:
Reliable, long-duration power remains a constraint for distributed sensing systems, particularly when deployed in environments in which battery replacement is impractical. Power sources such as lithium batteries, solar panels or harvesting from ambient energy each have limitations relating to endurance, maintenance or environmental dependence. There is therefore strong motivation to explore **bio-derived, self-sustaining power systems** in which naturally occurring or engineered microorganisms generate electricity directly from soil or organic matter. Engineering-biology approaches, such as microbial fuel cells (MFCs) or soil microbial fuel cells (SMFCs), offer compelling alternatives. These systems harness the metabolic activity of electrogenic bacteria found within soil or an organic substrate, passing the electrons they release through an external circuit to generate electricity. Recent work [1] has field-demonstrated proof-of-concept systems capable of powering water purification.

Significant limitations remain, however, including low power density, variable output, stability whilst operating under field conditions and the challenge of interfacing with IoT electronics or power-management systems. The goal of this research topic is to develop and test **engineering-biology power systems** that can power IoT devices sustainably under real-world conditions.

Unclassified Example Approaches:
- **Microbial/biological engineering** [2]: Identify, engineer or enrich electrogenic microorganisms (e.g. Geobacter, Clostridiaceae) for improved current output, stability in variable environments and compatibility with low-nutrient or waste-substrate operation.
- **Electrode and materials engineering** [3]: Develop novel electrode materials (e.g. bio-char, activated carbon from biomass waste, carbon felt/stainless steel composites) and architectures (i.e. electrode spacing, surface area, stack configuration) to optimise electron transfer and durability of microbial fuel cells.
- **Power harvesting and electronics integration**: Design or adapt low-voltage, low-current energy-harvesting circuits and power-management systems to better suit the output characteristics of MFCs, suitable for powering power IoT sensor nodes, data logging or wireless communications. Field-deployment and sustainability assessment: Test MFC systems under realistic or tactical conditions (e.g. outdoor, variable soils and temperatures), evaluate long-term performance, maintenance needs, environmental impacts and lifecycle sustainability. Explore techniques such as stacking of cells and modular design to scale output and increase robustness.
- **Application demonstration** [7]: Implement a demonstrator IoT node (sensor or communication device) powered by a microbial battery, measure operational lifetime, reliability and feasibility in a resource-constrained scenario.

Unclassified Relevance to the Intelligence Community:
Sustainable power sources, requiring minimal maintenance, can enable a strategic advantage when operating in denied environments. A viable microbial-fuel-cell battery could support:

- **Autonomous sensor networks** in remote locations where battery replacement or routine maintenance is impractical, maximising intelligence coverage through continuous operation.
- **Sustainable and biodegradable power systems**, aligning with environmental and logistical resilience considerations.
- **Innovation in edge computing and power autonomy**, enabling sensor nodes and devices with extended lifetimes, independent of grid- or meteorologically sourced energy.

By combining engineering biology, materials science and electronics, this research aims to deliver a long-running, deployable and sustainable power solution for the next generation of low-power devices.

References:

[1] Dziegielowski, J, "*Development of a functional stack of soil microbial fuel cells to power a water treatment reactor: From the lab to field trials in North East Brazil*" Applied Energy (2020)
[2] Jiang, Y-B, "*Characterization of Electricity Generated by Soil in Microbial Fuel Cells and the Isolation of Soil Source Exoelectrogenic Bacteria*" Front Microbiol (2016)
[3] Mutuma, B, "*Valorization of biodigestor plant waste in electrodes for supercapacitors and microbial fuel cells*" Chemical Physics (2021)
[4] Hess-Dunlop, A, "*Towards Deep Learning for Predicting Microbial Fuel Cell Energy Output*" Electrical Engineering and Systems Science (2024)
[5] Dziegielowski, J, "*Towards effective energy harvesting from stacks of soil microbial fuel cells*" Journal of Power Sources (2021)
[6] Hess-Dunlop et al., "*Time-series forecasting of MFC energy generation using deep learning*" Front Comput Sci (2025)
[7] Kim et al., "*Development of a self-powered soil sensor using soil MFCs for power autonomous sensors for smart agriculture*" J. Power Sources (2026)

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.

NIEA-2027-011

Unclassified Research Topic Title:
Advancing risk assessment capabilities and understanding of LLMs and biological design tools

Unclassified Key Words:
artificial intelligence; large language models; biological design tools; membership inference attacks; unlearning; privacy and data security

Unclassified Research Topic Description, including Problem Statement:
The convergence of life sciences with big data and artificial intelligence has led to a surge in publicly released models. These models may originate from peer-reviewed publications, preprints, commercial products, or open repositories such as GitHub, and may be released as either closed- or open-weight models. As more large language models (LLMs) and biological design tools (BDTs) are released, it is essential that capabilities to assess and benchmark these models are also advanced—particularly in relation to information security, biosecurity, and biodefense.

Recent research indicates that LLMs and BDTs are vulnerable to privacy and integrity failures, similar to those initially observed in natural language processing and computer vision systems. Research avenues such as membership inference, overparameterization, prompt protection, and unlearning are actively being explored to characterize and mitigate these vulnerabilities. Advancing understanding of these and other risks in large pretrained models and generative diffusion models commonly used in life sciences is essential.

Unclassified Example Approaches:
- Develop membership inference and model inversion techniques specifically tailored to BDTs, and build tools to analyse data leakage in biological sequence and structural datasets used for model training.
- Investigate risks associated with imbalanced training and/or overparameterization in LLMs and BDTs, particularly in domains dominated by positive (published) data. Incorporate negative, null, and non-reproducible data—such as methods sections from peer-reviewed papers—into model evaluation.
- Advance the understanding of risks and opportunities associated with unlearning by developing scalable, provable, and adaptable methods for life science LLMs and BDTs.
- Develop processes, pipelines, and metrics to effectively and automatically baseline the capabilities of newly released LLMs and BDTs. Assessments should focus on shifts in the risk landscape outlined above, increased potential for misuse by malicious actors, and the emergence of novel, revolutionary capabilities not present in existing models.
- Security for Agentic Bio-Design: Develop safety protocols for autonomous AI agents, particularly those bridging the gap between computational models (LLMs/BDTs) and automated wet-lab infrastructure.
- Mechanistic Interpretability for Biology Models: Advance methods to decode the internal logic of BDTs and frontier models, ensuring we can distinguish between valid biological reasoning and dangerous dataset artifacts.

Unclassified Relevance to the Intelligence Community:

The intersection of AI and the life sciences is reshaping what is possible and is increasingly valuable to society - industry, governments and the research sector. The vulnerability of LLMs and BDTs to privacy and integrity failure raises unique national security, ethical and privacy challenges. These rapidly evolving concerns stand to be better understood.

Reference:

- Tang, X., Jin, Q., Zhu, K. *et al.* Risks of AI scientists: prioritizing safeguarding over autonomy. *Nat Commun* **16**, 8317 (2025). https://doi.org/10.1038/s41467-025-63913-1
- Rivera, S. and Mackelprang, R. Risk Mitigation for Biological Design Tools. *Engineering Biology Research Consortium.* September 2025. https://doi.org/10.25498/E4R10S

When preparing proposals please be duly respectful of:

- Australia's international obligations regarding the *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention)*; and
- Legislative sanctions frameworks under the *Charter of the United Nations Act 1945*, regulation instruments made under the *Charter of the United Nations Act 1945*; the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011*.
- Consideration must be given to ensure proposals are not open to misinterpretation, and do not put at risk Australia's long-standing commitment and reputation.