National Intelligence Postdoctoral Grant – Research Topics 2026

Reference	Topic Title
NIPG-2026-001	RISCV exploitation techniques and state of the market
NIPG-2026-002	Decoding money laundering activities using topographic maps and artificial intelligence
NIPG-2026-003	Forecasting climate change impacts on health security in the Indo-Pacific - national security implications for Australia
NIPG-2026-004	The human factor in cyber security resilience
NIPG-2026-005	The psychology of influence: Effective persuasion in the cybercrime ecosystem
NIPG-2026-006	Security evaluation of system-on-chip field programmable gate array designs against remote power side channel attacks
NIPG-2026-007	Loyalty in the Australian context
NIPG-2026-008	Using AI in psychological continuous assessment
NIPG-2026-009	The impact of artificial intelligence and machine learning on chemical and biological counter-measures
NIPG-2026-010	Rapid detection and identification of environmental pathogens
NIPG-2026-011	Enhancing intelligence benefits from suspicious activity reporting and analysis
NIPG-2026-012	Anti-authority ideological radicalisation and violence
NIPG-2026-013	Person-related misinformation as a strategic threat: understanding and mitigating its impact
NIPG-2026-014	Algorithmic recommender-based radicalisation and offline behaviour
NIPG-2026-015	Multifunctional metamaterials for broadband absorption of high-power microwaves
NIPG-2026-016	Creating cryptographic protocols with mature, diverse and performant quantum resistance
NIPG-2026-017	Engineering biology for sustainable power generation
NIPG-2026-018	Bio-inspired molecular sensors for adaptive computing and environmental intelligence

*** Bold = agency proposed topic**

NIPG-2026-001

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.

NIPG-2026-002

Unclassified Research Topic Title:
Decoding money laundering activities using topographic maps and artificial intelligence

Unclassified Key Words:
Money laundering; cryptocurrency mixers; financial intelligence; Web3; cross-chain bridges

Unclassified Research Topic Description, including Problem Statement:
The rapid growth of the Web3 ecosystem drives innovation but also generates opportunities for complex financial crimes. Over $2.8 billion has been stolen from cross-chain protocols, accounting for nearly 40% of all Web3 hacks [1]. Siloed investigative tools that focus on individual blockchains are decreasingly useful. Pseudo-anonymity, immutability and cross-chain interoperability features in distributed ledger technologies introduce unique challenges to businesses and regulatory authorities. This often leads to laundering through illicit services. Criminals may use cryptocurrency mixers and tumblers to conceal transaction trails. This chain—from an exploit on a bridge to illicit activity on a mixer—emphasizes the need for a unified intelligence framework to analyse the entire attack lifecycle, rather than just its components.

Cryptocurrency mixers break the links between transaction inputs and outputs by pooling funds from users. They are exploited for illicit finance, laundering proceeds from hacks, ransomware, and crimes. The shutdown of centralized mixers, such as ChipMixer [2], and sanctions on decentralized ones, like Tornado Cash [3], demonstrate law enforcement efforts to disrupt them. However, an ongoing 'cat-and-mouse' game persists. Modern mixers can utilize sophisticated techniques to evade forensic detection, making construction of provenance more challenging. This demands intelligence systems that learn and identify new obfuscation patterns.

Cross-chain bridges are also prime targets for attacks due to the large sums they manage. Early attacks, such as the Ronin Bridge hack, resulted in over $600 million being stolen [4] due to a private key compromise. More recently, attackers exploited deep code flaws in Wormhole and Nomad bridges [5], using logic errors to bypass verification and drain funds.

A new generation of tools is needed for intelligence agencies, financial institutions and law enforcement authorities to address emerging challenges in detecting, tracking and prosecuting money laundering activities.

Unclassified Example Approaches:
Approaches can include:

- Novel framework(s) to reconstruct provenance and detect suspicious entities.
- Feature extraction and detection mechanisms capable of detecting interrelated vulnerabilities and system risks in Web3 systems.
- Advanced data analytics algorithms to exploit hidden connections and reveal the linkages to automatically reconstruct the provenance, i.e. asset flows and payment histories of suspicious activities in almost real-time.
- Use of big data analytics tools, graph-embedding and 3D topographical attribute mapping.

Unclassified Relevance to the Intelligence Community:
This addresses the challenges in detecting money laundering activities through cryptocurrency mixers. Benefits include a new generation of tools for financial institutions and law enforcement authorities, enhancing cyber infrastructure resilience and a novel integrated system capable of detecting fraud and proactively identifying vulnerabilities in the NextGen Finternet.

References:

1. Seven Key Cross-Chain Bridge Vulnerabilities Explained. https://chain.link/education-hub/cross-chain-bridge-vulnerabilities
2. Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and Other Assets. https://www.justice.gov/usao-ndtx/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other
3. The Tornado Cash Delisting and Sanctions Compliance Implications for Crypto. https://www.k2integrity.com/en/knowledge/policy-alerts/the-tornado-cash-delisting-and-sanctions-compliance-implications-for-crypto/
4. Ronin Network: What a $600m hack says about the state of crypto. https://www.bbc.com/news/technology-60933174
5. Nomad Loses $156 Million in Seventh Major Crypto Bridge Exploit of 2022. https://www.elliptic.co/blog/analysis/nomad-loses-156-million-in-seventh-major-crypto-bridge-exploit-of-2022

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.

NIPG-2026-003

Unclassified Research Topic Title:
Forecasting climate change impacts on health security in the Indo-Pacific - national security implications

Unclassified Key Words:
Health security; climate change; national security; Indo-Pacific

Unclassified Research Topic Description, including Problem Statement:
Health security refers to the activities and measures taken at the global, national, regional and local level to ensure the protection of human health against threats or events that could cause harm. These measures focus on a broad range of health threats including emerging and re-emerging infectious diseases with the potential to cause epidemics and pandemics, bioterrorism, disasters (natural and man-made), and accidental or intentional release of chemical, biological, radiological and nuclear (CBRN) agents that threaten health.

Communicable disease outbreaks, disasters, and weak health systems pose risks not only to public health, but also to regional and global economies and security. In addition to creating new and hard to predict crises for public health systems and other government agencies, public health challenges can exacerbate health inequalities, magnify socio-economic and political instability, and threaten national and regional security and stability. Adverse health conditions may also enable the recruitment of disenfranchised and vulnerable individuals by violent extremists and for foreign interference.

Climate change is altering rainfall and temperature patterns and increasing the frequency and severity of weather events. The resultant changes in the geographical distribution of communicable disease pathogens and their vectors are predicted to expose people, animals and plants to new biological agents. This poses a risk of decrease food- and water-security, further stress of health systems, and the exacerbation of health security issues in direct and indirect ways which are changing and not fully understood.

A systematic analysis of the intersection between climate change and health security elements, including distribution of communicable diseases and vectors, ability of the health system to prevent, detect and respond to disease outbreaks, the capability and capacity of the health infrastructure in the Indo-Pacific, and the subsequent development of forecasting and modelling techniques, will provide important current situational awareness (intelligence).

Unclassified Example Approaches:
This research would suit those undertaking research in epidemiology, public health, modelling (disease, economic, climate change, risk), with special respect to large language models and computational forecasting tools. Possible approaches include:

- Identification of existing and/or new indicators of impacts of climate change on health security elements and evaluate the degree to which these meaningfully measure the impact on national security.
- Assessment of forecasting and modelling tools to understand and model current and future impacts of climate change on health security elements that could constitute a significant risk to regional security in the Indo-Pacific and internationally to Australia.

- Development of systems to better leverage and collate existing and new data to inform more timely risk-informed analysis.
- Enhance the accessibility and use of surveillance data to support effective and evidence-based analysis by the National Intelligence Community.

Unclassified Relevance to the Intelligence Community:
Forecasting and modelling climate change impacts on health security in the Indo-Pacific and understanding the developing national security implications for Australia is needed to maintain situational awareness, inform intelligence products, and enhance national preparedness.

References:

- National Health and Climate Strategy
- The 2025 Global Report of the Lancet Countdown on Health and Climate Change
- World Bank 2024: Quantifying the Impact of Climate Change on Health in Low- and Middle-Income Countries
- Health risks of climate change in the 21 Pacific Island states and noted gaps in scientific evidence: A scoping review
- Human health and climate change in the Pacific: a review of current knowledge
- To prepare for future threats, treat health security as national security | The Strategist
- Multilateral Health Partnerships: The Value of Australia's Support for Gavi and The Global Fund in the Indo-Pacific Region - Australian Global Health Alliance
- The geopolitics of climate and security in the Indo-Pacific - ASPI
- Enhancing health security - European Observatory on Health Systems and Policies

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.

NIPG-2026-004

Unclassified Research Topic Title:
The human factor in cybercrime resilience

Unclassified Key Words:
Cybercrime prevention; cyber security; social engineering; behavioural science; data science

Unclassified Research Topic Description, including Problem Statement:
Despite billions invested into cybersecurity globally, cybercrime continues to rise at significant rates. In Australia, scams, phishing, fraud and social engineering account for the majority of reported incidents, with annual losses measured at an average of $30,700 per report, across over 87,400 individual reports (Australian Signals Directorate, 2024). Most incidents occur not through technical intrusions, but by exploiting human vulnerabilities. Cybercrime offenders rely on trust manipulation, social engineering and psychological biases to defraud individuals and businesses.

There is a critical need for deeper insight into the human factor in cybercrime (Dupont & Holt, 2022). Humans are part of the solution to cybercrime so how can we incorporate behavioural insights, and user experience design, to decrease cyber victimisation? Similar to how road safety campaigns made seatbelts and drink-driving awareness part of everyday culture, we need systemic, behavioural strategies to make individuals and organisations more resilient to cybercrime.

Unclassified Example Approaches:
1. Psychology of victimisation and resilience
    - What makes some individuals or organisations fall for scams repeatedly, while others resist?
    - Role of trust, risk perception, stress, and cognitive biases in cybercrime susceptibility.
    - Use surveys, interviews, and vignette experiments to compare groups.
2. Behavioural interventions and nudges
    - Testing real-time interventions: pop-up warnings, scam filters, transaction holds with contextual advice.
    - Large-scale randomised controlled trials with banks, telcos, or government platforms.
3. Human-centered design of systems
    - Embedding scam-resistant UX/UI into digital services (e.g., email, banking, government apps).
    - Usability studies and co-design workshops with at-risk groups (seniors, small businesses, CALD communities).

Unclassified Relevance to the Intelligence Community:
This project aligns with two National Intelligence Community (NIC) research priorities:
- Human Behaviour and Influence
- Cyber Security, Protective Security and Physical Security

By examining the psychological and social drivers of cybercrime victimisation and resilience, the research advances understanding of how cybercrime actors exploit human behaviour to execute criminal operations at scale. The project also contributes to national cyber security efforts by

developing proactive, human-centered prevention strategies that complement technical defences. This two-pronged approach strengthens the NIC's capacity to anticipate, detect, and mitigate cyber threats to the Australian community.

References:

- Akdemir and Lawless (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.
- Australian Signals Directorate (2024). *Annual Cyber Threat Report 2023-2024.* https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
- Back and LaPrade, (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *Future*, *9*, 6-2019.
- Bada *et al.* (2023). *An evaluation of police interventions for cybercrime prevention* (No. UCAM-CL-TR-983). University of Cambridge, Computer Laboratory.
- Dupont and Holt (2022). The human factor of cybercrime. *Social science computer review*, *40*(4), 860-864.
- Jeong *et al.* (2019). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th international conference on collaboration and internet computing (CIC)* (pp. 338-345). IEEE.
- Näsi *et al.* (2023). Cybercrime victimisation and polyvictimisation in Finland—prevalence and risk factors. *European journal on criminal policy and research*, *29*(2), 283-301.
- Nurse (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

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.

NIPG-2026-005

Unclassified Research Topic Title:
The psychology of influence: Effective persuasion in the cybercrime ecosystem

Unclassified Key Words:
Offensive cyber; online behaviour; persuasion psychology; social psychology; online influence

Unclassified Research Topic Description, including Problem Statement:
There is a growing literature supporting the efficacy of influence strategies in the online environment (Costello *et al*., 2024; Simchon *et al.*, 2024). More recently, academic interest has centered on how large-scale personalised persuasion can be achieved based on psychological and environmental factors (Hackenberg *et al*., 2025; Matz *et al*., 2024). The proposed project draws on this evidence base connecting the psychology of persuasion with advances in large language models (LLMs) to address the problem statement "What evidence-based persuasion and influence techniques are effective to shape behaviour in a cybercrime ecosystem?" Combining this knowledge, this project aims to proactively influence and achieve behaviour change within the cybercrime ecosystem. This is a shift from traditional cybercrime strategies that prioritise defensive systems. Rather the proposal seeks to develop and optimise scalable offensive approaches to provide disruption opportunities, shape disengagement and proactively discourage cybercrime.

Unclassified Example Approaches:
1. Developing and testing models using persuasive dialogue interventions powered by LLMs.
2. Explore the efficacy of using Artificial Intelligence (AI) to generate persuasive content based on psychological and linguistic understandings of a cybercrime environment.
3. Develop a framework to test and examine the efficacy of persuasion strategies in the cybercrime ecosystem through linguistic and psychological insights.
4. Apply knowledge of hacker communities (or malicious cyber actors) to understand narrative discourse to inform behaviour change.
5. Optimise the scale, speed and personalisation of proactive online influence strategies.
6. Identify cybercrime populations most vulnerable to behaviour change and influence to then develop targeted interventions for disengagement.

Unclassified Relevance to the Intelligence Community:
Australia is a significant target for cybercriminals including both opportunistic and state-sponsored actors. While significant resources underpin Australia's defence systems against cybercrime attacks, less attention has been paid to how Australia may engage in offensive efforts targeting cybercrime. Cybercrime is technologically enabled human action. Understanding the people and the ecosystems that allow cybercrime to thrive is essential in identifying potential avenues for offensive operations. Using advances in AI and LLM technology to understand large amounts of data, research in online influence and the psychology of persuasion, as well as generative AI-enabled content provides opportunities in the future for advancing an offensive approach to targeting cybercriminals. This research will assist in developing evidenced-based capabilities for the National Intelligence Community.

References:

- Costello, T. H., Pennycook, G., & Rand, D. G. (2024). Durably reducing conspiracy beliefs through dialogues with AI. *Science*, *385*(6714), eadq1814. DOI: 10.1126/science.adq1814
- Hackenburg, K., Ibrahim, L., Tappin, B. M., & Tsakiris, M. (2025). Comparing the persuasiveness of role-playing large language models and human experts on polarized US political issues. *AI & SOCIETY*, 1-11. https://doi.org/10.1007/s00146-025-02464-x
- Matz, S. C., Teeny, J. D., Vaid, S. S., Peters, H., Harari, G. M., & Cerf, M. (2024). The potential of generative AI for personalized persuasion at scale. *Scientific Reports*, *14*(1), 4692. https://doi.org/10.1038/s41598-024-53755-0
- Simchon, A., Edwards, M., & Lewandowsky, S. (2024). The persuasive effects of political microtargeting in the age of generative artificial intelligence. *PNAS nexus*, *3*(2), pgae035. https://doi.org/10.1093/pnasnexus/pgae035

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.

NIPG-2026-006

Unclassified Research Topic Title:
Security evaluation of system-on-chip field programmable gate array designs against remote power side channel attacks

Unclassified Key Words:
FPGA based, System-on-Chip (SoC)

Unclassified Research Topic Description, including Problem Statement:
With current advancement in embedded systems, field programmable gate array (FPGAs) and CPUs are usually integrated as discrete components, and are thus implemented as separate chips on board. The processor and the FPGA communicate through an off-chip bus and may share main memory (DRAM). However, due to small footprint and lower power consumption requirements, the hardware vendors such as Xilinx and Intel have introduced heterogeneous system-on-chip (SoC) FPGA designs, which integrate both processing cores and FPGA fabric in one silicon die [1,2,4]. These integrated FPGA designs introduce new security vulnerabilities that can be exploited to perform power side-channel analysis, without physically accessing or being in the proximity of the target device [1,4].

Consider a SoC-FPGA architecture that contains both processing core (CPUs and GPUs) and FPGA fabric in one silicon die, and the system has proper protection mechanism to prevent direct accesses from an FPGA fabric to the rest of the system. Also, assume that the attacker cannot be in physical proximity of the target device. In this scenario, an attacker can instantiate ring oscillators (ROs), or a delay line coupled with time-to-digital converters (TDCs) to measure the voltage fluctuations on the shared power distribution network (PDN) that are caused by the target circuit [4-6]. Because an FPGA is programmed by loading a bit-stream in software, an adversary who has access to bit-stream data, or has permission to program at least a part of an FPGA, can perform power side-channel attacks remotely. This attack vector can also be applicable to discrete FPGA architecture that shares the same power supply with a CPU on the system, or data-centres that allows multiple users to co-share the FPGA resources [7,8].

For heterogeneous SoC-FPGA architectures, it is common for modules on the same die to share the same power supply. For example, in Xilinx Zynq SoC both CPU and FPGA fabric share the same PDN. The PDN converts and distributes power from the power supply to individual circuit components (in this case CPU and FPGA fabric), with a goal to provide a clean voltage supply resistant to varying current demands [3,4].

To maintain a constant voltage, a PDN uses a voltage regulator to adjust the amount of supplied current and uses decoupling capacitors as a buffer to handle current variations. However, the voltage regulator and the decoupling capacitors cannot completely hide current variations, and high switching activities often lead to transient voltage drops in the PDN of an FPGA [3]. The voltage drop on the PDN reflects the power consumption [3]. Additionally, a change in the combinational logic delay reflects the voltage drop that correlates with the power consumption and the switching activity of the circuits [3]. This correlation between combinational logic delay and the power consumption can be leveraged to build an on-chip power monitor that will allows us to measure a combinational path delay, and further estimate the power consumption of other modules that share the PDN [3].

The FPGA based on-chip power monitors are typically either TDCs or ROs. Both circuits exploit propagation delay as a proxy for measuring supply voltage, as lower supply voltage is known to

cause an increase in the propagation delay [9]. TDCs detect voltage changes in the FPGA PDN by sensing changes in the delay of a propagating signal through a chain of buffers or other logic [9,12]. TDC sensors can also be used as receivers for covert communication from information leaking hardware Trojans in the target circuit [9,12]. ROs based sensors can also be used to monitor the supply voltage of an FPGA PDN because the propagation delay through the RO, which depends on supply voltage, can be observed by measuring oscillation frequency [10,11].

Unclassified Example Approaches:

- Identify different power monitors and compare with existing ROs and TDCs power monitors.
- Investigate different ROs designs for power monitoring and estimate their entropies.
- Validate the capability of remote power side-channel attacks against modern FPGA architectures.
- Develop countermeasures against remote power side channel attacks.

Unclassified Relevance to the Intelligence Community:

This research will inform understanding and confidence in FPGA based SoC designs, characterise potential remote power side channel attacks and inform potential mitigation strategies.

References:

1. Trimberger and McNeil, "Security of FPGAs in data centers," in 2017 IEEE 2nd International Verification and Security Workshop (IVSW), 2017
2. Gnad, et al. "Voltage drop-based fault attacks on FPGAs using valid bitstreams," in 27th International Conference on Field Programmable Logic and Applications (FPL), 2017.
3. Pant, "Design and analysis of power distribution networks in VLSI circuits," Ph.D. dissertation, The University of Michigan, 2008.
4. Masle and Luk, "Detecting power attacks on reconfigurable hardware," in 22nd International Conference on Field Programmable Logic and Applications (FPL), 2012.
5. Barbareschi et.al., Implementation and Analysis of Ring Oscillator Circuits on Xilinx FPGAs. Springer International Publishing, 2017.
6. Hoque, "Ring oscillator based hardware trojan detection," Master's thesis, University of Toledo, Toledo, Ohio, USA, 2015.
7. Amazon EC2 F1, https://aws.amazon.com/ec2/instance-types/f1/ , Amazon.com, Inc, accessed: 2017.
8. Chen et al. "Enabling FPGAs in the cloud," in 11th ACM Conference on Computing Frontiers (CF), 2014.
9. Dennis et al. 2016. Analysis of transient voltage fluctuations in FPGAs. In International Conference on Field-Programmable Technology.
10. Zhao and Suh. 2018. FPGA-based remote power side-channel attacks. In 2018 IEEE Symposium on Security and Privacy (SP'18). IEEE.
11. Kenneth and Hayes. 2012. Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems. ACM Transactions on Reconfigurable Technology and Systems 5, 1 (2012).
12. Kenneth and French. 2013. Sensing nanosecond-scale voltage attacks and natural transients in FPGAs. In ACM/SIGDA International Symposium on Field Programmable Gate Arrays.

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.

NIPG-2026-007

Unclassified Research Topic Title:
Loyalty in the modern Australian context

Unclassified Key Words:
Loyalty, loyalty vs disloyalty, organisational identity, culture, demographics

Unclassified Research Topic Description, including Problem Statement:
The Australian Government's sensitive resources, information and facilities must be protected if they are to remain effective. Security clearances are a key component of the protective security apparatus. Individuals who are granted these clearances must demonstrate high levels of integrity and must be loyal to Australia and its democratic system of government. Loyalty is a key consideration explored through recruitment and security clearance vetting processes before an individual commences employment. Once an individual is employed, their loyalty is continuously assessed throughout the lifecycle of their clearance and employment within their organisation.

While the security vetting processes provide a framework to assess an individual's loyalty, this has typically been applied in a dualistic manner. Clearance subjects are assessed to be loyal or disloyal with no further nuance, and this assessment is often extrapolated to all aspects of their life – including loyalty to their country, their employer, and in their personal relationships. However, as can be seen in international examples, some perpetrators of insider acts, including espionage, have claimed unwavering loyalty to their country even after they have been prosecuted. This does not appear consistent with the behaviour of a loyal individual. As such, a dualistic approach to assessing loyalty may be limited in the modern Australian environment and could place the Government's sensitive resources at increased risk of compromise.

The modern Australian environment includes the changing dynamic of Australia's multicultural and demographic profile. Australia is becoming an increasingly multicultural country, with a higher proportion of first-generation Australians making up the workforce. These individuals may retain a sense of loyalty (e.g. cultural) to their country or place of origin, and potentially may not meet the required standard of loyalty in a personnel security assessment. It also appears that the generational differences between young early-career employees and their older, established colleagues are becoming increasingly stark. Younger employees are typically pursuing multiple shorter term career opportunities and are changing employers more frequently than older employees. These younger individuals could be described as 'disloyal' through current personnel security assessment practices. As the cultural and demographic dynamics of Australia's workforce continue to change, Governments may face an increasingly restricted pool of employment candidates assessed by traditional means as suitably loyal for access to classified material.

This proposes research into concepts of loyalty, and their application to the personnel security context, to support personnel security assessment processes. The research aims to inform Government processes remain attuned to Australia's current cultural and demographic profiles and may be appropriately adjusted as these profiles continue to change in future. We propose the research focuses on the broad categories below:

- Definitions and concepts of loyalty, including its philosophical and psychological underpinnings and how this has changed over time.

- How loyalty is conceptualised and experienced by individuals from diverse cultural backgrounds and/or from different generations, and whether this aligns with current approaches to assessing loyalty.
- Implications of the above in the Australian personnel security context, including considerations for organisational identity, whether loyalty is an effective assessment tool, and if there are alternatives to loyalty that provide more value in personnel security assessments.

Desirable topics to explore in the personnel security/insider threat context include:

- Nested and multifaceted loyalties.
- Methods to objectively define and measure loyalty – is loyalty simply the absence of disloyalty and/or betrayal, or can it be measured with more accuracy?
- Is there an ideal range of loyalty for clearance holders – can an employee be too loyal?
- The interaction between entitlement, ego and loyalty to self.

Unclassified Example Approaches:

- Literature review to orient the researcher. This will probably involve exploring different definitions of loyalty and their underlying philosophical or psychological frameworks.
- Analysis of insider threat case studies to allow the researcher to examine different concepts of loyalty and their manifestation in insider threat cases. All kinds of insider threat cases should be considered, including those without an obvious nexus to loyalty to a country.
- Interviews with personnel security/insider threat practitioners, and insider threat specialists. Interviews will give the researcher an understanding of how practitioners in the field apply concepts of loyalty when assessing clearance suitability and managing ongoing and emerging employee risk the workplace. This approach could attune the researcher to what is currently being done, enabling a more nuanced consideration of what research indicates and what is practicable in the workplace.

Unclassified Relevance to the Intelligence Community:

This research will support the work being undertaken by the NIC relating to the management of insider risk.

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.

NIPG-2026-008

Unclassified Research Topic Title:
Artificial intelligence (AI) in personnel security psychological assessments: exploring and examining technological capabilities to strengthen Australia's protective security.

Unclassified Key Words:
Personality assessments, machine learning, psycholinguistic analytics, continuous assessment, cognitive and behavioural concerns.

Unclassified Research Topic Description, including Problem Statement:
The Australian Government's most sensitive resources, information and facilities must be protected if they are to remain effective. Security clearances are a key component of the Australian Government's protective security apparatus. Individuals who are granted these clearances must demonstrate high levels of integrity, be trustworthy, and be committed to Australia, its values, and its democratic system of government. The clearance assessment process determines ongoing clearance suitability through initial security reviews and continuous assessment throughout the lifecycle of the clearance. Integral to both elements of the clearance assessment process are psychological assessments.

Psychological assessments for security clearance suitability examine an individual's overall psychological functioning and identify psychological vulnerabilities associated with insider threat. This is a necessary and comprehensive component of robust clearance assessment, resulting in a level of assurance that is critical to protecting the Australian Government's most sensitive resources.

However, the ability to recruit and maintain appropriately qualified and experienced psychologists in a strained labour market and in the context of increasing demand by the Australian Government to deliver clearances is a challenge. AI solutions may have the potential to assist workforce processes through early identification of candidates that present with high levels of insider threat risk, thereby streamlining the workflow for more comprehensive components of the clearance assessment process (including the psychological assessment). AI solutions may also assist in enhancing the identification and analysis of risk based on data collected through comprehensive, point in time assessments as part of the clearance process (including the psychological assessment). Further to this, there may be applications that support the ongoing/continuous assessment and management of clearance holders.

Against this context, the increasing availability of high-dimensional and fine-grained data about human behaviour gathered from online sources – such as social media posts, text messages and emails – has the potential to augment the way psychologists perform personality assessment. Personality traits have been shown to predict a broad range of life outcomes in the domains of health, political participation, personal romantic relationships, interpersonal functioning, purchasing behaviours, and academic and job performance as well as insider threat indicators. These new sources of data may provide additional insights about an individual's personality traits that enhance traditional psychological assessments. Furthermore, this could potentially increase insight into the day-to-day functioning of clearance subjects, providing greater assurance about the subject's ongoing suitability to access highly sensitive material. Leveraging this data may also present an opportunity for the automated and sustained psychological

assessment of clearance subjects, potentially reducing workforce demand while increasing real-time coverage. However, the introduction of sophisticated and intrusive initial and continuous evaluation tools may raise questions about privacy and consent.

This topic proposes research into applications of AI to support initial and continuous psychological assessment processes. The research aims to support the development of technologies that will assist personnel security psychologists, analysts and insider threat specialists to proactively identify and analyse risk to prevent insider acts. Specific consideration should also be given to examining the ethical and review implications of using AI to support the psychological assessment process. We propose the research focus on the three components of the psychological assessment process in personnel security:

- Initial psychological assessment (scheduled point in time assessment).
- Interval-based ongoing psychological assessment (scheduled point in time assessment).
- Real-time detection of known cognitive and behavioural concerns as identified in malicious insider threat research.

Unclassified Example Approaches:
Conduct a meta-analysis of past studies using machine learning (ML) and psycholinguistic analytics in personnel psychology to illuminate the benefits and challenges in building, interpreting, and validating ML models applied to psychological assessment for security purposes.

Unclassified Relevance to the Intelligence Community:
The proposed research would support the current activities of the NIC. It would inform the continued modernisation and enhance future capabilities by exploring AI applications to psychological assessments both during initial processes and through ongoing continuous assessment.

References:

- Du Xiaowei and Sun Yunmei (2022) 'Linguistic features and psychological states: A machine-learning based approach', *Frontiers in Psychology,* DOI: 10.3389/fpsyg.2022.955850.

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.

NIPG-2026-009

Unclassified Research Topic Title:
The Impact of Artificial Intelligence and Machine Learning on Chemical and Biological Warfare

Unclassified Key Words:
Artificial intelligence, drug design, pharmacology, machine learning, neural networks, algorithm, MegaSyn, BioNavi, Chemistry42, proteomics, computational biology, synthetic biology, chemical weapons, biological weapons

Unclassified Research Topic Description, including Problem Statement:
Artificial intelligence (AI) enabled tools are expanding the scope of chemical and biological sciences. Previously unknown molecules and organisms are now being discovered and previously unreachable molecules are becoming more accessible. AI enabled tools are being deployed in the pharmaceutical industry, biotechnology and genetic engineering, consumer product manufacturing (cosmetics, avoidance of animal testing and to reduce environmental impacts), and in agriculture (biodegradation and reducing toxicity to non-target species). This broad-ranging scientific trend may also be used to design or produce new chemical and biological structures similar or superior to known chemical and biological warfare (CBW) agents. The potential capacity for rapid growth of available CBW threats with enhanced or comparable lethality to presently known toxic agents could potentially overwhelm international arms controls and countermeasure capability and will require the proactive development of new surveillance methods and novel detection, identification and mitigation systems.

Applicants should approach the topic with intent of undertaking a literature review and feasibility analysis of predictive AI algorithm applications and trends with respect to potential impacts on chemical and biological warfare controls.

Unclassified Example Approaches:
Research proposals could approach this issue from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of chemistry, biotechnology, synthetic biology, computer/software engineering, neural networks and machine learning (ML), applied science, innovation policy, and pharmacology. Proposals may consider ways to monitor and mitigate threats of generatively designed agents using:

- machine learning models that use publicly available datasets and open-source generative software
- additional machine learning tools to model parameters such as environmental and metabolic stability
- retrosynthesis tools (commercially available or open-source)
- identification of suitable “chemistry/biology starting points”

Unclassified Relevance to the Intelligence Community:
Artificial intelligence-based generative design is a disruptive (emergent and convergent) technology with the potential to generate new threat agents, or increase the threat from current agents. The combination of technological advances in this field, coupled with the limited regulations associated with rapidly developing AI technologies, may result in proliferation of AI-enhanced threats. A deeper understanding of the latest technological improvements in the AI and ML fields, the potential applications of AI/ML in a CBW context, and the prospects of

technologies to protect/defend against these applications, are critical to informing warnings and indicators for the intelligence community.

Information relevance to the intelligence community could be prioritised as follows (according to technology maturity):

1. Safeguard implications for artificial intelligence enhanced CBW agent design. The dual-use nature of artificial generative design technology advancements and potential impacts on chemical and biological threats.
2. Safeguard implications for technological/design hurdles from theoretical to practical design outputs – including; current limitations of AI/ML systems, overcoming predictive failure and computational structure validation challenges, and future impacts of quantum machine learning.
3. Safeguard implications of adaptive AI/ML to develop strategies and materials to proactively avoid controls, detection and countermeasures.

Understanding these emerging technological possibilities will lay the knowledge foundations to provide the NIC with the insight necessary to address risks associated with the field in terms of national security and global proliferation.

References:

- De Lima RC, Sinclair L, Megger R, Maciel MAG, Vasconcelos PFDC, Quaresma JAS. Artificial intelligence challenges in the face of biological threats: emerging catastrophic risks for public health. Front Artif Intell. 2024 May 10;7:1382356. doi: 10.3389/frai.2024.1382356.

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.

NIPG-2026-010

Unclassified Research Topic Title:
Rapid Detection and identification of environmental pathogens

Unclassified Key Words:
Environmental pathogen, genome, DNA sequence, real-time sequencing, diagnostics, bio-surveillance

Unclassified Research Topic Description, including Problem Statement:
Environmental pathogens are estimated to cost Australia billions of dollars every year, through causing human disease, endangering native animal and plant species, or damaging the environment and agricultural ecosystems. Plant pathogens pose significant threats to agricultural output, while human pathogens can cost millions more in financial losses in healthcare and lost worker productivity. Their effects include lost production, environmental damage, and the endangerment of native species. Some pathogens can also cost millions more in healthcare and lost productivity.

Microbial pathogens (bacteria, viruses and some fungi) cannot be readily detected and accurately identified in the environment, at the point of exposure. In these cases, samples are sent to a laboratory for analysis – a relatively slow and inefficient process that may yield inconclusive results depending on sample quality, sample preparation and handling, and technological post processing.

Identifying microbial or viral environmental pathogens in a way that is rapid, accurate and sensitive remains a challenge. Identification would likely require a broad-spectrum assay that includes the ability to identify unique genetic signatures for accurate strain identification. However, this capability would have broad applicability for bio-surveillance and safety in various industries such as agriculture, food safety and healthcare.

This project aims to explore state-of-the-art methods, so that control and oversight authorities are equipped to detect and accurately identify pathogenic microorganisms in the environment. Future technology should be adjustable to allow new species to be added to the control pool in order to keep up with the rapid evolution (or development i.e. through genetic engineering) of new species of microbes and viruses of concern.

Applicants should approach the topic with intent of undertaking a literature review and feasibility analysis of current and emerging technologies and processes for the detection and identification of environmental pathogens that inhabit all domains (air, water and land). Then, through research and analysis, determine how such technologies, equipment or processes can be optimised for rapid and accurate detection at the point of exposure to environmental pathogens.

Unclassified Example Approaches:
Research proposals could approach this issue from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of biotechnology, genomics, synthetic biology and engineering. The proposal should focus on exploring new platform capability for the detection and identification of a range of pathogenic microorganisms, but could initially focus on

the detection and identification of a single pathogen with high selectivity and sensitivity with the potential to broaden the platform in the future. Investigations could include a range of novel methodologies.

Unclassified Relevance to the Intelligence Community:
The national security implications of environmental pathogen detection and identification are significant. At the national level, insight into such emerging technologies would better enable the NIC to monitor and report on the spread of human or crop diseases. Detection of pathogens is critical for strategic and operational awareness; and for assigning accountability under international treaties, peace agreements and global norms.

References:

- Xu, J., M. Akhtar, W. Meng, J. Bai, S. Prince, and R. Huang. 2025. " Advances in Pathogen Detection: From Traditional Methods to Nanotechnology, Biosensing and AI Integration." *Wiley Interdisciplinary Reviews: Nanomedicine and Nanobiotechnology* 17, no. 4: e70022. https://doi.org/10.1002/wnan.70022.

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.

NIPG-2026-011

Unclassified Research Topic Title:
Enhancing intelligence benefits from suspicious activity reporting and analysis

Unclassified Key Words:
Suspicious activity reporting; suspicious matter reports

Unclassified Research Topic Description, including Problem Statement:
All sectors of Australia including the public, government, academia, business and industry have roles to play in safeguarding Australia's national security, protecting Australians, and preserving sovereign capability, commercial, social, environmental and scientific advantages. Suspicious activity reporting is a critical and powerful tool used by the National Intelligence Community (NIC) and broader government to achieve this.

Suspicious activity reporting is used to report activities that may indicate criminal behaviour and threats to national security including terrorism, espionage, insider threat, foreign interference, fraud, money laundering, illicit drugs and scams. Whilst some information must be reported under legislation (e.g. financial transactions by financial institutes) most reporting is voluntary. The information provided is triaged, assessed, and used to provide valuable intelligence for NIC agencies. Examples of suspicious activity reporting tools in use include those at AUSTRAC, Home Affairs, Crime Stoppers, ASIO and the National Security Hotline. Reporting has traditionally been via phone and website both at the National and State/Territory level.

To maximise intelligence benefits from suspicious activity reporting, high-quality, accurate and timely reporting from all demographics and sectors is required, along with community awareness on what constitutes, and how to report, suspicious activity with respect to national security. Efficient downstream processes for triaging and developing intelligence leads are also required; ideally capable of pulling and assimilating data from multiple State and National reporting tools. Adherence to legislative protections, such as privacy and permissions, is critical.

Unclassified Example Approaches:
Opportunities for research include:

- Psychological, social, technological and contextual factors that motivate reporting.
- Educational approaches and/or tool(s) to encourage reporting quality; frequency, evidence, accuracy, data.
- Assessment of mechanisms of reporting to ensure fit for purpose for all demographics and national security crime types, including newer forms of suspicious activities (e.g. radicalisation, anti-authority ideologies, insider threats and foreign interference).
- Use of AI and large language models to triage, assess and develop intelligence insights from reporting datasets and multiple sources.
- Basic data collection to inform Australian circumstances (e.g. where, how and by whom is it being reported, who is not reporting, what types of activities and/aren't being reported).

Unclassified Relevance to the Intelligence Community:
Addressing these knowledge gaps is critical for current situational awareness and maximising the timely reporting of, and actionable intelligence leads from, suspicious activities. This provides

early indicators to safeguard national security and protect Australian citizens and sovereign capability.

References:

- https://www.austrac.gov.au/business/core-guidance/reporting/suspicious-matter-reports-smrs
- https://www.homeaffairs.gov.au/about-us/what-we-do/borderwatch/reporting
- https://crimestoppers.com.au/
- https://nitro.asio.gov.au/
- https://www.nationalsecurity.gov.au/what-can-i-do/report-suspicious-behaviour

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.

NIPG-2026-012

Unclassified Research Topic Title:
Anti-authority ideological radicalisation and violence

Unclassified Key Words:
Anti-authority; Anti-Australia; Anti-government ideology; Anti-community; violent extremism; mixed ideology; sovereign citizens; neo-Nazis; cookers.

Unclassified Research Topic Description, including Problem Statement:
Anti-authority (Commonwealth, State and/or local; parliaments and agencies) ideology, extremism and conspiratorial social groups, such as the Australian sovereign citizen self-identifiers, has existed in Australia for decades with beliefs loosely manifested in individuals and online groups finding ways to dissociate from societal structures, including living off-grid and in isolation. However, in Australia, and internationally, there has been a growth in the movement along with a shift to clearer organisation, leadership, connection, recruitment and overlapping with other groups (e.g. anti-vax groups, conspiracy groups, far-right/left extremist, manosphere, and familiar abusers).

Stemming from anti-government, anti-establishment and anti-social beliefs, self-identifiers consider themselves not subject to certain laws and refuse to comply with some processes including paying taxes, undertaking random breath tests and obeying road rules. At the same time, they are supporters and users of government services, such as Medicare and income support. There is a propensity for fixation on high office holders, public figures and law enforcement, which has culminated in acts of violence, including deaths of Police Officers.

It is possible the frequency and severity of anti-authority ideological radicalisation fuelled violence in Australia may increase, along with risks to national security. Understanding these developing dynamics is the subject of this topic.

Unclassified Example Approaches:
Opportunities for research include:

- Psychological, social and contextual factors that make some anti-authority ideological radicals more likely to be violent than others.
- Radicalisation pathways and threat markers for violent offending.
- Basic data collection to inform Australian circumstances.
- Risk factors for radicalisation of anti-authority ideological radicalisation.
- Factors that make law enforcement targets for anti-authority ideological radicals.
- Risks to national security from foreign interference exploitation of anti-authority ideological radicalisation.
- Assessment of forecasting and modelling tools to understand and model current and future impacts of anti-authority ideological radicalisation that could constitute a significant risk to national security in Australia.

Unclassified Relevance to the Intelligence Community:
Addressing these knowledge gaps is critical for ongoing situational awareness and providing early indicators to safeguard national security, in particular the safety of the general public,

public office holders and law enforcement officers. The research would equip the NIC with insight into anti-authority ideological radicalisation associated radicalisation and violence.

References:

- Participation in anti-authority protests and vulnerability to radicalisation | Australian Institute of Criminology
- Violent extremism in Australia: An overview | Australian Institute of Criminology
- Anti-Government Extremism in Australia: Understanding the Australian Anti-Lockdown Freedom Movement as a Complex Anti-Government Social Movement Understanding the Australian Anti-Lockdown Freedom Movement as a Complex Anti-Government Social Movement on JSTOR
- What Is Anti-Government Extremism? on JSTOR
- Australian Government, *A Safer Australia: Australia's Counter-Terrorism and Violent Extremism Strategy* (Canberra: Australian Government, 2025) https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/australias-counter-terrorism-violent-extremism-strategy.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.

NIPG-2026-013

Unclassified Research Topic Title:
Person-related misinformation as a strategic threat: understanding and mitigating its impact

Unclassified Key Words:
Continued influence effect; person-related misinformation; human behaviour and influence

Unclassified Research Topic Description, including Problem Statement:
Despite increasing scholarly attention to misinformation, we lack a clear understanding of why person-related misinformation—false claims targeting individuals or social groups—continues to influence beliefs and behaviours even after it has been corrected. This persistence, known as the continued influence effect, is concerning. Person-related misinformation not only distorts factual understanding but also reinforces harmful stereotypes, exacerbates intergroup tensions, increases polarisation, and threatens democratic and social cohesion.

Person-related misinformation can be deliberately weaponised by hostile actors seeking to exploit identity-based tensions. For example, disinformation campaigns like Russia's use of opposing "Black Lives Matter" and "White Lives Matter" narratives illustrate how such content can be engineered to provoke outgroup derogation, fuel radicalisation, and incite societal unrest.

Despite its strategic threat, the field remains unclear on why person-related misinformation is so resilient—persisting in memory and influencing judgements after correction, and the impacts of this to Australia's national security.

Unclassified Example Approaches:
Research opportunities include:

- Psychological, social and contextual factors that allow person-related misinformation to persist following a correction.
- Understanding which individuals and groups are most susceptible, and under what conditions.
- Message features—such as emotional salience or alignment with stereotypes— that make this type of misinformation especially resistant to correction.
- Understanding how person-related misinformation interacts with social identity, stigma, and perceived threat to amplify its influence.
- Opportunities to counter the continued influence effect.
- Basic data collection to inform Australian circumstances.
- Risks to national security from person-related misinformation.
- Assessment of forecasting and modelling tools to understand and model current and future impacts of person-related misinformation that could constitute a significant risk to national security in Australia.

Unclassified Relevance to the Intelligence Community:
Addressing these knowledge gaps is critical to strengthening societal resilience, safeguarding vulnerable communities, and providing insight for the NIC on influence operations that threaten Australia's social cohesion and democratic integrity.

References:

- Ecker *et al.* The psychological drivers of misinformation belief and its resistance to correction. Nat Rev Psychol 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y
- Why Misinformation Must Not Be Ignored. https://psycnet.apa.org/fulltext/2025-57011-001.html
- Thinking clearly about misinformation https://www.nature.com/articles/s44271-023-00054-5
- Exploring factors that mitigate the continued influence of misinformation https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-021-00335-9
- Continued Influence of Misinformation and the Information Disorder https://academic.oup.com/book/59599/chapter-abstract/503181045?redirectedFrom=fulltext&login=false
- Mechanisms in continued influence: The impact of misinformation corrections on source perceptions https://link.springer.com/article/10.3758/s13421-023-01402-w
- Bennett *et al*. (2024). Alert, but not alarmed: Electoral disinformation and trust during the 2023 Australian Voice to Parliament Referendum. Policy & Internet. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.429
- Lewandowsky *et al*. (2023). Misinformation and the epistemic integrity of democracy. Current Opinion in Psychology. https://www.sciencedirect.com/science/article/pii/S2352250X23001562
- Ross *et al*. (2022). Russian meddling in U.S. elections: Disinformation and democratic vulnerability. Mass Communication and Society. https://www.tandfonline.com/doi/full/10.1080/15205436.2022.2119871
- Vosoughi *et al.* (2018). The spread of true and false news online. *Science*. https://www.science.org/doi/10.1126/science.aap9559

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.

NIPG-2026-014

Unclassified Research Topic Title:
Algorithmic recommender-based radicalisation and offline behaviour

Unclassified Key Words:
Algorithmic radicalization; violent extremism; gender; misogyny; terrorism; Australia

Unclassified Research Topic Description, including Problem Statement:
While Australia has experienced fewer terrorist attacks compared to other Western nations, several significant violent incidents committed in Australia, or by Australians over the past several years, reflect the various forms of violent extremism that permeate Australian consciousness. Analyses of these incidents, which include the 2015 Lindt Café siege, the 2019 Christchurch Mosque attacks, and both the Bondi Junction and Wakeley Church stabbing incidents in 2024, have established that the majority were influenced by factors connected to gender and/or racial ideologies.

Attention to what might be described as pre-cursor content (that which is ideologically aligned with extremist beliefs, but does not explicitly promote or endorse them), is notably absent in extant examinations of this phenomenon. Critically, in a fundamental departure from intentional engagement with these beliefs on traditional web forums or groups e.g., reddit, this content may be – but is not necessarily sought out by the user. Algorithmically driven content consumption common on platforms such as Facebook, Instagram, YouTube and TikTok diminishes individual user autonomy and exposes them to ideas they may never have searched for in the first place.

Users are seldom shown extremist content in initial platform interactions. Rather, exposure to and engagement with more subtle content that reflects extremist ideology (e.g., sexist content, anti-vax content) boosts contact with overtly extreme, violent or radical content over time (e.g., Beecham *et al*., 2021; Mamié *et al*., 2021; Rowa, 2022; Weiss *et al*., 2024). The extent to which these trends are reflected among Australian users is poorly understood, as these studies addressed specific geographic cohorts outside Australia, or did not examine or specify the geographic makeup of their sample. Algorithmic exposure to more overtly extreme content has been observed to foster further autonomous engagement (Weiss *et al*., 2024), which can promote migration to more dedicated extremist "fringe" spaces (Mamié *et al*., 2021).

Unclassified Example Approaches:
While a relationship between radicalisation and exposure to harmful online content has been observed elsewhere (e.g., Mamié *et al*., 2021; Weiss *et al*., 2024), this has not been thoroughly assessed in the Australian population. Similarly absent from extant research is a consideration of the impacts relatively innocuous (but ideologically aligned) content may have in this context. Noting the extant challenges impeding effective understanding and response to this issue – such as profit driven resistance to reform, and erroneous ascription of "exposure", research proposals are invited that may examine the following in the Australian context from a psychosocial perspective:

- Is there a relationship between algorithmic recommender-based radicalization and offline behaviour?
- How do these processes work in instances where extreme offline behaviour materialises?
- What factors mediate exposure (passive engagement) to this content;
- What factors mediate active engagement with this content;

- What factors drive progression to viewing more extreme content;
- What factors promote migration to other online spaces that overtly promote extremism.

This research would provide insight into the characteristics of who is most susceptible to this (precursor and borderline/grey) content and why, and the process by which this phenomenon impacts upon further autonomous engagement and offline action.

Unclassified Relevance to the Intelligence Community:
Insight into the processes by which algorithmic recommender-based radicalisation relates to offline behaviour would provide the NIC with improved understanding of emerging radicalisation dynamics. Exploration of this phenomenon in Australia, based upon Australian data, provides current context and situational awareness.

References:

- Cole, J., Alison, E., Cole, B., & Alison, L. (2010). Guidance for identifying people vulnerable to recruitment into violent extremism. Liverpool, UK: University of Liverpool, School of Psychology.
- Corner, E., Gill, P., Schouten, R., & Farnham, F. (2018). Mental disorders, personality traits, and grievance-fueled targeted violence: the evidence base and implications for research and practice. Journal of personality assessment, 100(5), 459-470.
- Doosje, B., Loseman, A., & Van Den Bos, K. (2013). Determinants of radicalization of Islamic youth in the Netherlands: Personal uncertainty, perceived injustice, and perceived group threat. Journal of Social Issues, 69(3), 586-604
- Egan, V., Cole, J., Cole, B., Alison, L., Alison, E., Waring, S., & Elntib, S. (2016). Can you identify violent extremists using a screening checklist and open-source intelligence alone? Journal of Threat Assessment and Management, 3(1), 21.
- Gill, P., Horgan, J., & Deckert, P. (2014). Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. Journal of forensic sciences, 59(2), 425-435.
- Holt, T. J., Freilich, J. D., Chermak, S. M., Mills, C., & Silva, J. (2019). Loners, colleagues, or peers? Assessing the social organization of radicalization. American Journal of Criminal Justice, 44(1), 83-105.
- Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. The ANNALS of the American Academy of Political and Social Science, 618(1), 80-94.
- Malthaner, S. (2017). Radicalization: The evolution of an analytical paradigm. European Journal of Sociology/Archives Européennes de Sociologie, 58(3), 369-401.
- McCauley, C., & Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. American Psychologist, 72(3), 205.
- Ozer, S., & Bertelsen, P. (2018). Capturing violent radicalization: Developing and validating scales measuring central aspects of radicalization. Scandinavian journal of psychology, 59(6), 653-660.
- Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT research paper, 97(1), 22.
- Webber, D., & Kruglanski, A. W. (2018). The social psychological makings of a terrorist. Current opinion in psychology, 19, 131-134.

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.

NIPG-2026-015

Unclassified Research Topic Title:
Multifunctional metamaterials for broadband absorption of high-power microwaves

Unclassified Keywords:
Multifunctional metamaterials; multi-physics simulations; electromagnetic absorption; system reliability; multi-material additive manufacturing

Unclassified Research Topic Description, including problem statement:
Emerging development and deployment of high-power microwave (HPM) weapons (Benford 2024) will likely increase the vulnerability of satellites, aircraft and terrestrial devices. Electromagnetic metamaterials, as artificially engineered structures, can be tailored to either absorb or reflect HPM, depending on their material compositions and structural configuration, which offer a promising route for improved device protection. Nevertheless, conventional electromagnetic metamaterials only exhibit narrowband protection and generally fail to address the coupled electromagnetic–thermal–mechanical interactions that occur under broadband HPM exposure. Such coupling effects can lead to localised overheating, material degradation, and mechanical instability, which in turn trigger cascading failures that pose threats to device survivability and reliability.

This interdisciplinary topic aims to develop multifunctional metamaterials (Li *et al.* 2022) that exhibit broadband electromagnetic performance, efficient thermal management, and enhanced mechanical stability to minimize the adverse effects of HPM on device survivability and reliability in a range of environments. The project would explore a new generative design approach that systematically integrates multi-physics simulations, advanced system reliability assessment methods, rational design optimisation approaches, and multi-materials additive manufacturing techniques to design multifunctional metamaterials for improving the survivability and reliability of devices against HPM threats.

Unclassified Example Approaches:
Possible approaches are:

- Conducting multi-physics simulations to investigate the coupled electromagnetic–thermal–mechanical behaviours of multifunctional metamaterials.
- Developing advanced rational design optimisation approaches to generate multifunctional metamaterials with broadband microwave absorption, efficient thermal management, and enhanced mechanical stability.
- Utilizing multi-material additive manufacturing techniques for prototyping and conducting experimental characterization of the electromagnetic, thermal, and mechanical properties of meta-lattices under HPM excitation.

Unclassified Relevance to the intelligence community:
This project would explore avenues for advanced materials technologies that may address emerging HPM threats to electronic devices. The project will experiment with multifunctional metamaterial systems capable of protecting devices against HPM threats, to enhance survivability and reliability of critical assets.

References:

- Benford J. History and future of high power microwaves[J]. IEEE Transactions on Plasma Science, 2024, 52(4): 1137-1144.
- Li Z, Gao W, Wang M Y, *et al*. Design of multi-material isotropic auxetic microlattices with zero thermal expansion[J]. Materials & Design, 2022, 222: 111051.
- Yang Y, Yin Z, Zhu X, *et al*. A review of multimaterial additively manufactured electronics and 4-D printing/origami shape-memory devices: Design, fabrication, and implementation[J]. Proceedings of the IEEE, 2024.

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.

NIPG-2026-016

Unclassified Research Topic Title:
Creating cryptographic protocols with mature, diverse and performant quantum resistance

Unclassified Key Words:
Post-quantum cryptography

Unclassified Research Topic Description, including Problem Statement:
The global research ecosystem has been effective at generating the core ideas for secure, post-quantum cryptographic primitives and protocols. As part of this work, notions have received varying levels of attention, such as:

- Maturity (i.e. does a post-quantum scheme exist for a given use-case? Are the security properties well studied?)
- Diversity (i.e. for any given cryptographic use-case, are multiple categories of hard-problems available for the basis of the cryptographic primitives?)
- Performance (i.e. is a given scheme practical in terms of computational and data bandwidth requirements?)

For example, the only National Institute of Standards and Technology (NIST) standardised key-encapsulation mechanism relies on the hardness of certain lattice problems while a second key-encapsulation mechanism relying on the hardness of a certain decoding problem has been chosen for future standardisation. While the level of NIST standardisation represents a very high level of maturity and performance, the two choices of hard problems represent a moderate level of diversity. For other use-cases, these three aspects have been explored to different levels.

This research topic seeks submissions to conduct research that will either:

- Enhance the maturity of existing post-quantum cryptographic primitives, including providing additional confidence in security claims.
- Provide additional diversity to the hard problems underlying cryptographic protocols in use-cases with limited diversity.
- Improve performance to post-quantum cryptographic protocols where that performance increase leads to applications that are currently unfeasible.

Unclassified Example Approaches:
Depending on the proposer's areas of interest, some steps in potential pathways include:

- Examine literature around existing standards to identify gaps in either maturity, diversity or performance.
- Enhance "advanced cryptography" (i.e. cryptographic use-cases not limited to basic confidentiality, authentication, integrity and non-repudiation; some examples include attribute based encryption, private information retrieval and private set intersection) that is still under active research.
- Investigate proposed mathematical approaches that may lead to diversity in post-quantum cryptographic primitives and protocols.

Note that the question of increased diversity is a fundamental question of mathematical discovery, while improving maturity and performance are more closely tied to cryptographic science and computational science respectively.

Unclassified Relevance to the Intelligence Community:
Increased diversity in available cryptography, while not necessarily needed, provides redundancy in the unlikely event that fundamental flaws arise in accepted primitives. Diversity may also allow for different trade-offs of externals such as computation and bandwidth which can be critical in increasing performance to acceptable levels for niche applications within the National Intelligence Community (NIC).

References:

- [NISTIR8547] National Institute for Standards and Technology (2024), Transition to Post-Quantum Cryptography Standards (Initial Public Draft), https://doi.org/10.6028/NIST.IR.8547.ipd
- [NISTIR8528] National Institute of Standards and Technology (2024), Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8528

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.

NIPG-2026-017

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. Therefore, there is 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.

However significant limitations remain, 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:** 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).

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.

NIPG-2026-018

Unclassified Research Topic Title:
Bio-inspired molecular sensors for adaptive computing and environmental intelligence

Unclassified Key Words:
Molecular sensing; synthetic biology; biomolecular computing; DNA/RNA logic; chemical reaction networks; adaptive systems; biosensor interfaces; low-power computing

Unclassified Research Topic Description, including Problem Statement:
Biological systems have evolved remarkable capabilities for sensing, processing and responding to complex environmental signals. From molecular recognition by nucleic acids to the self-regulating feedback of metabolic networks, biology offers rich examples of computation without silicon. Advances in molecular biology, synthetic chemistry and bioengineering now make it feasible to design molecular sensors that also compute; systems able to detect signals, process information and trigger responses autonomously.

Proposals should investigate bio-inspired molecular sensors; integrating sensing and computation at the molecular or cellular scale. The goal is to explore how these systems can enable adaptive, low-power intelligence in settings where traditional electronics cannot easily function, such as inside living systems, in extreme environments or in highly miniaturised platforms.

Of particular interest are systems that:
- Exploit DNA, RNA or protein logic circuits to perform computation on environmental or biological inputs.
- Combine molecular sensing and decision-making, enabling autonomous activation or suppression of downstream responses.
- Operate in challenging or resource-limited environments, where conventional sensors are unsuitable.
- Provide new routes to biological-electronic interfaces, allowing molecular information to be captured and acted upon in real time.

Unclassified Example Approaches:
Proposals may take experimental, simulation-based or hybrid approaches. Possible directions include:
- **Molecular Logic and Computation:** Design and characterise molecular circuits using DNA strand displacement, riboswitches, enzymatic networks or similar mechanisms, which perform logic or classification tasks in response to chemical stimuli.
- **Chemical Reaction Network Modelling:** Use CRN frameworks to model molecular computation and assess the robustness, scalability and energy efficiency of different network topologies.
- **Biohybrid Sensor Interfaces:** Integrate molecular sensors with electronic, optical or microfluidic platforms to achieve reliable signal transduction and data readout.
- **Synthetic Biology for Sensing:** Engineer living or cell-free systems to detect multiple analytes and perform programmable responses. Explore how gene circuits or metabolic pathways can implement logic gates, memory or feedback control.

- **Assurance and Verification:** Develop methods to verify, calibrate and stabilise molecular sensing systems, ensuring repeatability, robustness and security in operational environments.
- **Synthetic Cells and Partitions**: Investigating physical partitions in a functional network that require transport control mechanisms that manage/coordinate system behavior.

Unclassified Relevance to the Intelligence Community:
Molecular and bio-inspired sensors could underpin a new generation of adaptive intelligence systems: autonomous, low-power and capable of operating where silicon-based devices fail:

- **Environmental and Material Detection:** bio-computing sensors capable of recognising hazardous materials and autonomously classifying hazards, deployable with a very low probability of detection compared with electronic techniques.
- **Edge Computing at the Molecular Scale:** Distributed, self-powered systems performing local computation and decision-making in the field, reducing dependence on traditional compute infrastructure.

By merging molecular sensing and computation within biological substrates, this research aims to extend the boundaries of both molecular intelligence and biological computing, supporting intelligence capabilities that are adaptive, resilient and informed by the environment itself.

References:

- Yaxue Hu et. Al., "*Intelligent molecular logic computing toolkits: nucleic acid-based construction, functionality, and enhanced biosensing applications*", Chemical Science (2025). https://doi.org/10.1039/D5SC06176H
- Debopriya Bose et. Al., "*The logic devices for biomolecular computing: Progress, strategies, and future directions*", Nano Today (2024). https://doi.org/10.1016/j.nantod.2024.102320

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.