Australian Government | Office of National Intelligence

National Intelligence Discovery Grants (NIDG) Program

ID26: Intelligence Challenges 2026

The *2017 Independent Intelligence Review* identified a number of challenges facing Australia's intelligence enterprise over the coming decade. These included the increasing complexity of the geostrategic environment, broadening scope of national security and intelligence missions, rapid pace of scientific and technological change and high levels of innovation investment by other nations. To meet these challenges the Review recommended a more systematic approach to leveraging science and technology.

As part of a wider response package, the *National Intelligence Discovery Grants* (NIDG) were established in 2020 to provide a mechanism for academic engagement.

The *2024 Independent Intelligence Review* provides contemporary guidance including drawing awareness to certain emerging technologies (artificial intelligence, quantum computing, sensing and communications technologies, and synthetic biology) and the importance of climate change and misinformation and disinformation. It is recommended to review the *2024 Independent Intelligence Review*, particularly Chapter 13 (Technology).

The following nine challenges have been detailed for the *National Intelligence Discovery Grants* (NIDG) Program (ID26) to enable the National Intelligence Community (NIC) to leverage emerging science, technology and social science, for funding commencing in 2026.

1. Covert collection challenges

The ability to:

- Access and collect intelligence from people, imagery, signals, emanations, signatures, nodes, networks and transactions with a low probability of detection and/or attribution.
- Degrade or defeat adversary collection and cyber capabilities to safely move people, information and equipment into, out of, and through, environments with low signature and likelihood of detection and/or attribution.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Sensors, signatures, signals analysis, emanations and networks.
- Forensic methods to detect and analyse tampering or manipulation of satellite imagery and other remote sensing data.
- Computer network exploitation.
- Covert, secure and assured communications and internet traffic including attribution and decloaking or otherwise anonymised traffic (e.g. I2P).
- Financial intelligence including cryptocurrency, block-chain and distributed ledger technologies.
- Emerging encryption technology including homomorphic and quantum based.
- Quantum sensing, classical sensors and radio frequency engineering.

2. Space-based technology challenges

The ability to:

- Leverage low cost and innovative technological advancement in space-based and high-altitude capabilities in a timely manner to improve collection, communication and analysis capabilities.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Satellite communications, sensors and networks.
- Automation and on-board processing and analysis.
- Advanced materials.
- Space-based situation awareness.
- Technology forecasting: emerging, critical and disruptive technologies including deficiencies and/or strengths in Australian capabilities.

3. Identity management challenges

The ability to:

- Quickly, accurately and uniquely identify individuals from all types of data (online, surveillance, biometric, speech, behavioural, forensic, text, etc.), including where the data has low linkages to real world identities.
- Mask or obfuscate the identity of an individual from adversaries where access to online, surveillance, biometric, forensic or other data is available.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Biometrics, biological or behavioural (e.g. gait analysis) for authentication, biometric authentication mechanisms and counter biometric considerations.
- Bio- and geo- forensics (including for law enforcement and prosecutions).
- Deep fakes/synthetic content analysis, detection and countermeasures.
- Web-scraping and machine learning for identity data.
- Socio-technical systems and systems integration.
- Named entity recognition using probabilistic methods.
- Identity verification processes for financial intelligence.
- Awareness and management of consumer data collection.

4. Emerging biological science challenges

The ability to:

- Develop methodologies, techniques, services and devices from emerging biological technologies to provide new or alternate options to meet existing and future intelligence mission objectives.
- Detect, identify, analyse, counter, defeat and prosecute threats from emerging biological technologies which have the potential to cause harm or detrimentally impact other organisms, materials, or infrastructure.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Emerging biotechnology and applications (e.g. in molecular biology, microbiology, immunology, virology, chemical sciences).
- Synthetic biology (e.g. genetic engineering, emerging threats).

- Bioconvergence - Quantum biotechnology, bio-based computing, (e.g. DNA-based data storage) and biohybrid materials (e.g. electronics, sensors etc).
- Bioenergy innovations.
- Pathogen threat detection, surveillance, modelling and countermeasures.
- Human augmentation technologies (e.g. neuroscience advancements, human-machine interface and wearable devices).
- New/novel forecasting techniques to enhance intelligence and national security (e.g. health, environment, CBRN).

5. Emerging material science challenges

The ability to:

- Develop methodologies, techniques, services and devices from emerging material technologies to provide new or alternate options to meet existing and future intelligence mission objectives.
- Identify, develop and/or employ new or novel materials with unique properties, including rare earths and complex alloys, to gain technical, performance and cost benefits.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Nanotechnology (e.g. miniaturisation and new functions).
- Emerging semi-conductor and related technologies.
- Power sources and batteries.
- Precision manufacturing, material science and cryogenics.
- Convergence or integration of technologies (e.g. nano-, bio- and info- technologies).
- Human augmentation technologies (e.g. human-machine interface and wearable devices).
- Quantum sensing and supporting technologies.
- Quantum material science and engineering related computing.

6. Cyber security, protective security and physical security challenges

The ability to:

- Ensure the security and integrity of sensitive and classified information through the hardening of physical, information, personnel and cyber security practices.
- Predict, prevent, detect, attribute, respond and recover from major incidents and malign online interference (foreign, domestic) at a national scale.
- Conduct cyber and informational activities to disrupt emerging security threats.
- Proactively detect and respond to insider threat behaviours of concern.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Cyber and national infrastructure systems analysis, vulnerability, risk and resilience.
- Human aspects of cyber security (e.g. behavioural analysis, sentiment analysis).
- Mobile device trust/assurance for remote access and collaborative working.
- Networking and sensor technologies including internet-of-things (e.g. LoRaWAN or related technology).
- Supply chain integrity, verification, optimisation and security (e.g. blockchain intelligence and insight into emerging digital currency management tools).
- Cryptography including crypt architecture, crypt engineering/implementation and side channel analysis.
- Crypto-jacking prevention and forensic science.

- Novel models for achieving rapid high assurance certification, accreditation and deployment of technologies for high secure networks and systems.
- Emerging quantum technologies to support security practices.
- Cyber extortion (e.g. ransomware) response and countermeasures.
- Dual design to incorporate both security/privacy and lawful access.
- Insider threat detection to proactively flag and identify concerns.
- The future of secure facilities and information security management.

7. Human behaviour and influence challenges

The ability to:

- Identify and understand actors and bystanders' psychologies, social identities, narratives and behaviours that constitute a threat to Australia's security.
- Mitigate and counter the cultural, psycho-social and organisational drivers and antecedents to national security threats.
- Influence target audiences to elicit information, affect behaviour or shape preferences.
- Understand the evolving nature of insider risk in the light of changing social and societal norms and the evolving risk landscape.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Identifying and countering malign foreign and/or domestic interference, influence and disinformation.
- Identifying trends in transnational, serious and organised criminal activities.
- Identifying and/or understanding drivers, antecedents and pathways to radicalisation and extremism (e.g. misogyny, environment).
- Understanding actors, communities, cultures, identities and narratives, and influencing effects/outcomes.
- Understanding, detecting and countering adverse 'crowd' or mass behaviour.
- Understanding human vulnerabilities related to cyber-extortion, trafficking, bribery and corruption.
- Behavioural analysis (e.g. NLP and language agnostic) of individual and group actors, including in person, online and via multi-source data to profile and predict psychological phenomena (e.g. motivation, intent, loyalty, trust).
- Predictive behavioural analysis of bystanders in response to complex scenarios (e.g. anticipating how someone will react, credibility of responses).
- Building trust and influence and eliciting information, including influencing outcomes in cross-cultural, hostile, resistant, conversational and time-sensitive contexts (in person and online), elicitation and credibility assessments.
- Resilience and functioning when alone/remote in oppressive or extreme environments.
- Insider risk indicators (e.g. culture or other drivers of why insiders do and don't betray trust, impact of emerging productivity tools, and management strategies).
- How deep or strategic fakes influence decision making and/or disrupt social norms.

8. Data-driven and real-time analytical challenges

The ability to:

- Employ advanced machine learning and data science techniques to autonomously (or semi-autonomously) identify, extract, fuse and disseminate meaningful intelligence from large, disparate, sparse and/or incomplete data sets (including linguistic, geospatial, financial, signals, identity and other relevant data) at the speed and scale required to meet emerging threats.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- Data management, data security, data assurance, data engineering and data curation.
- Automated information fusion, filtering, triage and knowledge management.
- Advanced sampling, pattern recognition, predictive analytics and statistics.
- Natural language processing, large language models and other language technologies.
- Financial intelligence analytics using large language models.
- Human-systems integration and uncertainty analysis.
- Techniques to account for human factors (e.g. errors, biases) in the interpretation and use of data.
- Quantum information sciences, including quantum algorithm development and post-quantum computing techniques.
- Emerging ubiquitous technical surveillance technologies and dynamics.

9. Situation awareness and multi-source assessment challenges

The ability to:

- Analyse and assess significant events and trends that impact on Australia's national security and interests (including political, strategic, environmental, economic, CBRN, as well as trends in adversarial behaviour, capability or investment in science, technology and social science).
- Collaboratively analyse and synthesise evidence from multiple sources, and across multiple agencies, to produce timely, high quality and influential intelligence reports and assessments.
- Articulate the basis and level of confidence in assessments.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities include:

- All-source intelligence integration and collaboration technologies.
- Political, strategic, economic and 'drivers of conflict' research and analysis including overt and covert propaganda and influence campaigns.
- New/novel technology forecasting for emerging, critical and disruptive technologies to enhance intelligence and national security (e.g. geospatial, geopolitical, health, CBRN) including deficiencies and/or strengths in Australian capabilities.
- National security implications of environmental change (e.g. forecasting certain climate change impacts) and health crises (e.g. epidemic, pandemic and agricultural impacts).
- Understanding and avoiding bias and generating confidence measures for assessments (e.g. reducing heuristic-based assessments when interpreting data to avoid skewed threat assessments).
- Enhancing cognition, comprehension, memory, learning and decision-making formally and in-the-field (e.g. visualisation).
- Identifying fundraising under false pretext to fund illicit activities (e.g. nefarious crowdsource fundraising).
- Emerging technology to enable fraudulent international transaction monitoring.
- Undersea / Deepsea situational awareness.