AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

SUBMISSION

Joint Standing Committee on the National Disability Insurance Scheme (NDIS) Inquiry into the Integrity of the NDIS

INTRODUCTION

The Australian Criminal Intelligence Commission (ACIC) welcomes the opportunity to provide a submission to the Joint Standing Committee on the National Disability Insurance Scheme (NDIS) Inquiry into the Integrity of the NDIS.

The ACIC is Australia's national criminal intelligence agency with an exclusive legislated mandate to combat serious and organised crime (SOC). The ACIC plays a central role in protecting Australia from criminal exploitation by providing high-quality criminal intelligence that informs operational decision-making, shapes policy and regulatory settings, and supports coordinated national responses across jurisdictions and sectors.

In fulfilling this role, the ACIC:

- provides unique, actionable and insightful criminal intelligence to partners and advice to government on SOC – including where it has a transnational dimension – through the collection and analysis of information and data on complex offending patterns, criminal business models, and criminal groups, networks and individuals across multiple crime vectors
- undertakes investigations and operations for purposes including identifying vulnerabilities in particular networks and systems, and collecting and disseminating intelligence – as well as evidence of SOC related offences – to facilitate enforcement, prevention, disruption and regulation activities
- provides national policing information systems and services to law enforcement and intelligence partners to keep them – and the Australian community – safe
- delivers background checking services to support employment or entitlement decisions and to maintain community safety.

THE EVOLVING SERIOUS AND ORGANISED CRIME ENVIRONMENT IMPACTING AUSTRALIA

Australia's SOC environment is becoming more complex, networked and damaging to the nation's economic, social and security interests. Contemporary SOC groups are highly opportunistic and increasingly diversified, targeting any activity where profit can be generated at scale, including the systematic exploitation of government-funded programs. This reflects a broader shift in the criminal landscape, with SOC increasingly converging with legitimate systems, services and supply chains, often supported by professional facilitators and corporate structures that obscure control and financial flows.

Today's SOC networks operate as decentralised, digitally enabled enterprises, frequently spanning multiple jurisdictions. Senior criminal figures may reside offshore while directing activity remotely through encrypted communications, digital platforms and trusted intermediaries. These networks rely on complex business structures and sophisticated financial arrangements to move and conceal proceeds, enabling them to adapt quickly to regulatory change and exploit vulnerabilities across both physical and digital environments. Technology has become a key enabler, allowing criminal groups to scale operations, reduce exposure and maintain resilience.

The scale of harm associated with this threat has grown significantly. The Australian Institute of Criminology estimates the cost of SOC to Australia reached up to $82.3 billion in 2023-24, equivalent to 3.2 per cent of GDP. Beyond direct economic losses, SOC activity undermines community safety, erodes trust in institutions, distorts legitimate markets and places sustained pressure on government services. As criminal enterprises increasingly embed themselves within lawful economic activity, they amplify systemic vulnerabilities and challenge traditional intelligence, regulatory and enforcement approaches.

In this environment, government-funded programs involving large public expenditure, complex delivery arrangements and vulnerable cohorts are particularly attractive targets. SOC actors actively seek opportunities where oversight can be circumvented, intermediaries leveraged and criminal activity disguised as legitimate service provision. Understanding this broader SOC context is critical to assessing non-compliance in the NDIS – fraud and 'sharp practices'[1] are not occurring in isolation, but as part of a wider criminal ecosystem that targets public funds and exploits structural weaknesses for profit.

Accordingly, addressing integrity risks in the NDIS requires an understanding of the contemporary SOC threat – one characterised by adaptability, convergence with legitimate systems and exploitation at scale. An intelligence-led approach that identifies emerging patterns, hidden

[1] Sharp practices refer to conduct that, while not necessarily unlawful, is deliberately misleading, exploitative or unethical, and designed to circumvent the intent of rules, safeguards or oversight mechanisms for improper advantage.

networks and cross-sector linkages is essential to supporting effective disruption, policy hardening and the long-term protection of the NDIS and its participants.

INTEGRITY OF THE NATIONAL DISABILITY INSURANCE SCHEME

ACIC intelligence indicates that non-compliance within the NDIS extends beyond isolated or opportunistic misuse and includes deliberate fraud, sharp practices and organised exploitation consistent with broader SOC methodologies. These behaviours have persisted over time and, in some cases, become increasingly sophisticated. Understanding the nature, extent and impacts of this SOC exploitation and non-compliance is critical to safeguarding participants, maintaining public confidence and protecting the long-term integrity of the NDIS.

Nature and extent of SOC exploitation and non-compliance, including fraud and sharp practices

Non-compliance within the NDIS occurs across a continuum, ranging from sharp practices at the margins of compliance to serious and organised fraud. Fraudulent conduct commonly includes false or inflated claims for supports that are not delivered, claims submitted while participants are hospitalised or incarcerated, and claims made against expired plans. In more serious cases, collusive arrangements have been identified between providers and participants, nominees or family members, including the provision of cash or other inducements to facilitate fraudulent access to the NDIS or ongoing misuse of participant plans.

The misuse of NDIS funds is a recurring feature of serious non-compliance. This includes large cash withdrawals, asset purchases and financial transactions that are inconsistent with the delivery of disability supports and indicative of efforts to obscure the origin or use of NDIS funds. Such conduct diverts funding away from intended supports, undermines the integrity of, and erodes public confidence in the NDIS.

Of particular concern is the involvement of SOC actors in exploiting the NDIS. The ACIC assesses that a range of criminal entities – including traditional organised crime groups, professional fraud syndicates and scheme-hopping networks – have established or infiltrated NDIS providers. These actors exploit the NDIS to generate income, launder illicit proceeds and conceal asset ownership, often using criminal business models observed across other Commonwealth payment and regulatory programs. This indicates that NDIS exploitation frequently forms part of broader, repeat offending rather than isolated misconduct. The money fraudulently obtained by SOC through exploitation of the NDIS is also routinely recycled into a range of other serious criminal activity.

A central enabling methodology is the use of cash incentives, or “kickbacks”, to participants, nominees or family members. These arrangements operate along a spectrum ranging from knowing collusion to coercion, and the ACIC assesses that some participants are likely unaware they are involved in fraudulent activity. In coercive cases, intimidation and threats of physical violence have been used to compel compliance, particularly against participants with physical or cognitive impairments.

Professional facilitation is a recurring feature of these exploitation models. In some cases, allied health professionals and other trusted intermediaries assist unsuitable providers to gain entry to the NDIS, pass audits or inflate participant funding, embedding sharp practices within otherwise legitimate professional and service delivery environments. This facilitation can include the preparation of false or exaggerated documentation to support access or higher funding, and materially increases the capacity of organised fraud actors to generate and sustain non-compliant activity within the NDIS.

While the precise quantum of fraud within the NDIS is difficult to accurately quantify, information suggests that the extent of non-compliance is significant and, in some cases, systemic. Analysis of providers subject to banning, suspension or serious regulatory action shows that a significant proportion exhibited historical risk indicators prior to entering the NDIS, including prior fraud convictions, adverse findings in other government programs, suspicious financial activity and poor engagement with the taxation system. In many cases, these indicators were identifiable before entry to the NDIS.

Impacts on participants and families

Non-compliance within the NDIS has direct and tangible impacts on participants and their families. Weaknesses in provider suitability and screening can allow unsuitable or criminally-linked providers to operate within the NDIS, increasing the risk that participants are exposed to poor-quality care, exploitation, or services that are not delivered as intended. Where oversight is limited and funding can be accessed without meaningful scrutiny, these risks are heightened, particularly for participants who rely heavily on providers to manage or deliver their supports.

Fraudulent and non-compliant conduct also diverts funding away from legitimate supports, undermining participants' safety, wellbeing and independence. In some cases, participants may be drawn into collusive arrangements – knowingly or unknowingly – exposing them to financial, legal and personal harm.

These harms are compounded where organised exploitation models rely on coercion. Participants from non-English speaking backgrounds, those with limited support networks, and those with significant physical or cognitive impairments may be particularly vulnerable. In coercive cases, intimidation or threats of violence can be used to compel compliance, undermining participants' ability to engage independently with the National Disability Insurance Agency (NDIA) and increasing the risk of ongoing harm.

Strengthening the integrity of the NDIS

Over time, a range of policy, regulatory and operational measures have been implemented to strengthen NDIS integrity, including enhanced compliance activity and increased inter-agency cooperation. The ACIC contributes to these efforts as a member of the Fraud Fusion Taskforce (FFT) and host of the Fraud Fusion Centre, which includes seconded members from various FFT agencies. The ACIC is working alongside partner agencies to integrate intelligence and regulatory information and target serious and organised fraud affecting the NDIS. These measures have improved the

detection and disruption of fraud, particularly among registered providers and cohorts identified as higher risk.

ACIC intelligence indicates that SOC actors continue to target perceived vulnerabilities within the broader NDIS integrity framework. In particular, structural features such as reliance on self-declaration and limited visibility of emerging risk during application processes can be exploited by SOC actors. Inability to effectively leverage adverse intelligence holdings or concerning patterns of behaviour, or verify self-disclosed information within suitability assessments may limit the effectiveness of timely intervention.

Similar challenges arise in relation to unregistered providers. Unregistered providers can lawfully deliver services to self-managed and plan-managed participants while operating outside many of the suitability, registration and ongoing compliance requirements that apply to registered providers. Given the scale of participant access to this cohort, unregistered providers may pose a real but not yet fully understood fraud risk. Reporting indicates that unregistered provider arrangements are frequently used by higher-risk actors to reduce scrutiny while maintaining access to NDIS funding.

Fraud risks in the NDIS are also evident in a broader, whole-of-government context. ACIC intelligence identifies repeat and cross-program offending, where individuals and networks previously subject to compliance or enforcement action in other Commonwealth programs subsequently re-emerge in the NDIS. This pattern highlights the challenges posed by fragmented information-sharing arrangements and the absence of a consolidated, cross-program view of provider risk and suitability frameworks.

Risks are most pronounced in parts of the NDIS where providers operate with limited checks or oversight, increasing exposure to repeat or organised non-compliance. In such contexts, approaches that improve visibility and monitoring – particularly where funding levels are high or delivery arrangements reduce transparency – may assist in reducing exploitation. More consistent consideration of relevant compliance, enforcement and historical risk information could further support earlier detection and prevention of these risks.

Continuing collaboration between agencies will enable opportunities to strengthen how the NDIS prevents exploitation, protects participants and reduces the risk of SOC involvement.

CONCLUSION

Non-compliance within the NDIS reflects the characteristics of a SOC threat environment in which criminal actors actively seek to exploit large, complex and well-funded public programs for profit.

Addressing these risks requires a sustained, intelligence-informed and coordinated approach across government. Effective protection of the NDIS depends on the ability to identify emerging patterns of exploitation, share relevant risk information across programs and jurisdictions, and intervene earlier to prevent harm to participants and misuse of public funds. Maintaining integrity settings that are intelligence-informed, risk-proportionate and responsive to changing threats is essential to protecting participants, maintaining public confidence and the long-term sustainability of the NDIS.

As Australia's national criminal intelligence agency, the ACIC will continue to support these efforts by providing intelligence on Australia's SOC threat environment to inform policy, regulatory and operational responses