Joint Committee of Public Accounts and Audit
Inquiry into the Administration of the

National Disability Insurance Scheme

The Committee will examine the National Disability Insurance Agency's (NDIA) delivery of the National Disability Insurance Scheme (NDIS) with reference to the management of financial sustainability risks and claimant and provider compliance with NDIS claim requirements; and the monitoring, measurement and reporting of NDIA performance.

The Committee will also examine the regulatory performance of the NDIS Quality and Safeguards Commission (NDIS Commission), and the Department of Health, Disability and Ageing's policy advice to the government.

Connecting a Decade of Failure

An AI-Powered Submission Revealing the Causes, Risks and Future Trajectory of the NDIS Crisis

By

Marie Johnson

December 2025

Table of Contents

Marie Johnson

Global Digital AI Authority | Author | Speaker | Adviser | AI Digital Human Inventor

Marie Johnson is a globally recognised authority on digital systems and Artificial Intelligence, with more than three decades of experience designing, governing and delivering large-scale national technology systems. Her career spans the earliest days of the Internet to contemporary AI-driven systems, with a sustained focus on how complex digital infrastructure shapes public administration, economic stability and human outcomes.

She is an award-winning international authority, author and in-demand speaker on Artificial Intelligence, digital government, digital humans, identity, cyber security, digital health, ethics, and the geopolitical consequences of national technology systems. Her work is distinguished by deep implementation experience across high-risk, high-impact environments - not theory or consultancy abstraction.

Marie is the author of two best-selling Amazon books on Artificial Intelligence. Including "*Nadia: Politics | Bigotry | Artificial Intelligence"*, which documented the creation and political termination of **Nadia**, the world's first AI-powered Digital Human co-created with people with disability. The work on Nadia helped catalyse a global AI Digital Human industry and remains a seminal case study in ethics, power, and technology governance.

Marie is also the inventor of the AI Digital Human Cardiac Coach, internationally acclaimed, piloted in health systems the United States, and the subject of Master of Computer Science thesis in the United Kingdom

In 2005, Marie was awarded the prestigious **United States Government O-1 Visa for Individuals of Extraordinary Ability** to take up a global role with Microsoft in Seattle, leading Microsoft's Worldwide Public Services and eGovernment industry. In support of the visa, Microsoft stated that *"Marie's e-government knowledge is unique in the world and is of particular interest to Microsoft as we pursue our e-government strategies."* Her work during this period focused on national digital government platforms and the strategic implications of public-sector technology at scale.

Across her career, Marie has advised governments and global organisations on the democratic, fiscal and human risks embedded in national digital systems. Her experience spans health and human services, disability services, immigration and visa systems, taxation, identity, payments, and global e-health.

Her senior roles have included Chief Information Officer, Chief Technology Architect, Technology Authority, intelligence analyst, board director and global adviser to governments. Early in her career, Marie worked in intelligence and analysis roles within the Australian Department of Defence, and later led the intelligence unit of an organised crime task force at the National Crime Authority. These roles shaped her deep understanding of systemic risk, enforcement complexity and the consequences of defective data and governance.

In the late 1990s, Marie led strategic intelligence, revenue forecasting and one of Australia's first major e-business initiatives at the Victorian State Revenue Office. That work delivered early electronic payments capability and was recognised internationally as one of the world's first successful e-business projects, later becoming a formal case study for executive programs at Melbourne Business School and INSEAD.

For five years, Marie led the **Business Entry Point,** an initiative of the thee levels of government in Australia. In 2000, in partnership with the Australian Tax Office, Marie led the delivery of the Australian Business Number registration process for millions of businesses ahead of the New Tax System. The introduction of the ABN established the foundation for business authentication in Australia This initiative is widely regarded as one of the most significant digital achievements in Australian public administration.

For many years, Marie served as **Chief Technology Architect for the Australian Department of Human Services**, with responsibility for architecture and technology business cases spanning the massive systems of Centrelink, Medicare Australia and the Child Support Agency. She initiated Payment Delivery Reform and led national and international consultation with the Reserve Bank of Australia and industry on innovation in payments and information services. She also served as Chief Technology Architect for the Australian Health and Human Services Access Card, developing global expertise in biometric identity systems for service delivery.

Marie's expertise in digital identity and payments informed the **2014 Australian Financial System Inquiry**, which recommended the introduction of a federated digital identity framework as critical to the resilience of Australia's financial system.

At the Department of Immigration and Citizenship, Marie designed and delivered the **Visa Pricing Transformation**, integrating digital channels, electronic payments and legislative reform, projecting an additional $700 million in revenue to the Federal Budget recognised internationally as a breakthrough in digital public administration. In partnership with Immigration and Citizenship Canada, Marie had executive responsibility for the delivery of the global **eMedical system**, enabling digital, risk-based health assessments across more than 100 countries.

Marie is the former **Head of the NDIA Technology Authority**. In that role, she was responsible for the original NDIS ICT business case, and shepherding the Business Case through the complex Australian Federal Budget process. Marie led the NDIA innovation program: the design and establishment of a network of solution design hubs; and the creation of Nadia before co-design was later abandoned by the Agency. She brings to this submission a rare combination of lived experience supporting family members with disability, deep internal knowledge of NDIA systems and culture, and extensive cross-government systems expertise.

Her board and advisory roles have included Independent Member of the Australian Federal Police Spectrum Program Board; member of the NSW Digital Government Advisory Board; invited member of the Accenture Global CIO Council; National Director of the Australian Information Industry Association; Faculty at Singularity University's Exponential Medicine program; and Inaugural Member of the ANU Cyber Institute Advisory Board.

Marie is a prolific writer and commentator, a regular contributor to national publications, and an internationally sought-after keynote speaker. Her work has been recognised through numerous awards, including a United Nations Public Service Award, Australian Innovative CIO of the Year, inclusion in Australia's *100 Women of Influence*, the Exceptional Woman of Excellence award at the Women Economic Forum, and the ACT Mental Health Carer Award.

Marie holds an MBA from Melbourne Business School (Innovation, Technology, eCommerce); a Bachelor of Arts (Military Strategic Studies, Geopolitical Complex Systems, International Relations); is a graduate of Harvard University John F Kennedy School Senior Executive Fellows Program; has undertaken tertiary studies in law; and is a Graduate of the Australian Institute of Company Directors.

Marie's lifelong interests include fitness, weight training and the NASA space program. Marie has run marathons including the London Marathon as part of a team of 10 raising $100,000 for the Leukaemia Foundation. Marie has visited the Kennedy Space Centre twice, including onsite to witness the launch of the last Space Shuttle Atlantis STS-135 in July 2011.

Statement of Standing and Expertise (Expert Evidence)

This submission is provided by **Marie Johnson** in the capacity of an **independent expert witness** on national digital systems, Artificial Intelligence, and large-scale public-sector service delivery.

Marie Johnson has more than **thirty years' professional experience** in the design, governance and delivery of nationally significant digital systems, including payment systems, identity systems, health and human services platforms, immigration and visa systems, and disability services. Her expertise arises from **direct responsibility for system design, implementation and operational risk**, rather than advisory, academic or consultancy commentary alone.

She has held senior executive and global leadership roles, including Chief Technology Architect, Technology Authority, Chief Information Officer, intelligence analyst, and board member, and has advised governments in Australia and internationally on the **systemic, fiscal and democratic risks** associated with national technology platforms.

Direct NDIA Expertise and Relevance to this Inquiry

Relevantly to this Inquiry, Marie Johnson is the **former Head of the NDIA Technology Authority**. In that role, she was responsible for:

- the original **NDIS ICT business case,** which **included cognitive intelligence** as a capability
- leading the Nadia project
- implementation of **co-design and innovation programs** aligned to the UN Convention on the Rights of Persons with Disabilities, and
- advising on the NDIA's technology operating model and cross-government system dependencies.

She therefore brings **first-hand internal knowledge** of NDIA systems capability, governance arrangements, operating culture, and the limitations of the Agency's ability to safely design and deliver complex digital reform. This knowledge is not retrospective or inferential; it is grounded in direct executive responsibility.

International Recognition of Extraordinary Expertise

Marie Johnson's standing as an expert in national digital systems has been formally recognised at the highest international level. In 2005, she was awarded the **United States Government O-1 Visa for Individuals with Extraordinary Ability**, to take up a senior global role with Microsoft in Seattle leading Microsoft's Worldwide Public Services and eGovernment industry.

In support of that visa, Microsoft stated: *"Marie's e-government knowledge is unique in the world and is of particular interest to Microsoft as we pursue our e-government strategies."*

The O-1 visa is granted only where sustained national or international acclaim and extraordinary ability are established. This recognition is directly relevant to the Committee's consideration of the weight to be given to her evidence on national systems failure.

Basis of Evidence

Marie Johnson's evidence is informed by:

- direct operational responsibility for systems of national scale
- internal NDIA knowledge and experience
- early-career roles in defence intelligence and organised crime task forces, shaping expertise in risk, enforcement and systemic complexity
- extensive analysis of official records including ANAO audits, Ombudsman reports, FOI disclosures, parliamentary inquiry materials, AAT decisions, procurement records and NDIA outage notices, and
- lived experience supporting family members with disability, providing insight into the real-world impacts of administrative and system failure.

She has made **multiple submissions to Parliamentary inquiries and oversight bodies over almost a decade,** warning of systemic risks within the NDIS, including unlawfulness, defective data structures, unsafe automation, governance failure and system instability. Those warnings have since been substantiated by documented outages, audits and operational failures now in the public record.

Independence and scope

The opinions and conclusions expressed in this submission are:

- **within her area of professional expertise**;
- based on **documented evidence and direct experience**;
- independent of the NDIA and the NDIS Quality and Safeguards Commission; and
- provided to assist the Committee in understanding matters of technical complexity, systemic risk and national consequence.

This submission is offered on the basis that the Committee may rely upon it as **expert evidence**, particularly in relation to national digital systems resilience; administrative law risk arising from system design; automation and algorithmic decision-making; governance and capability failure; and escalation of systemic failure to national economic impact.

Introduction. About this Submission

This submission is produced using an AI-powered system that I built and that operates entirely under my instruction. Every aspect of this submission has been generated, reviewed, edited and validated by me. This is the third such AI-powered system I have built.

The system is underpinned by an extraordinary, decade-long knowledge base comprising thousands of documents across the NDIS administrative landscape, including: FOI releases; ANAO audits; Ombudsman reports; Joint Standing Committee NDIS findings; NDIA system outage notices; AAT decisions; procurement records; academic research; independent expert commentary; and my own expert analyses. Significantly, this AI knowledge base includes all FOIs relating to the NDIA and NDIS Quality and Safeguards Commission that I have been able to identify and access.

For the first time, this material has been brought together into a single, connected, AI-driven analytical environment.

Nothing comparable exists within the NDIA, the NDIS Quality and Safeguards Commission, or the Commonwealth.

This provides the Parliament with something unprecedented: a complete, system-wide, decade-long view of risk within the NDIS national ecosystem and the administration of the NDIA. Patterns of failure, unlawful practices and systemic risk that were previously dispersed across agencies, reports and years of documentation are now visible as a coherent whole. What the NDIA has been unable or unwilling to recognise within its own operations for more than a decade is now clear, stark and unavoidable.

When examined collectively, the evidence establishes an **irrefutable national economic systemic crisis**. The failures identified are not confined to the NDIA or to the administration of the NDIS. They expose structural defects that place national expenditure, fiscal stability and the continuity of essential disability supports at direct and escalating risk.

For more than a decade, the Parliament and the public administration have examined fragments of this problem through audits, inquiries, reviews and complaints mechanisms. Yet these processes have operated in silos. None have been capable of knitting these findings together to identify the root causes of the crisis now confronting the nation.

This AI-powered system does exactly that.

Because the full picture is now visible - clearly, coherently and for the first time - the Parliament can no longer claim that the risks were unknown, unclear or unforeseeable. The consequences of inaction will not be confined to the NDIS. They will be felt across hospitals, State budgets, labour markets, regional economies and national fiscal stability.

This submission reveals a crisis that the NDIA lacked the capability or interest to see; that oversight bodies identified only in fragments; and that Parliament has never been shown in its entirety - until now.

The findings are not merely “alarming”.

They demonstrate a system sliding into **structural failure**.

They expose catastrophic defects at the core of the NDIA’s systems that threaten the continued functioning of the NDIS itself.

They reveal governance failures so serious that they now constitute a direct risk to national expenditure, participant safety and the integrity of public administration.

Executive Summary

Purpose of this Submission

This submission examines the administration of the National Disability Insurance Scheme (NDIS through the lens of its **systems, data, automation and governance**. It demonstrates that the most serious failures of the NDIS are not driven by participant behaviour or provider conduct, but by **systemic failures embedded in the digital and administrative foundations of the Scheme itself**.

The evidence establishes that the NDIS is becoming **incapable of operating as a coherent national system**, and that without urgent intervention it faces a **foreseeable collapse with national economic consequences**.

The Central Finding

The NDIS is failing because the NDIA's systems are failing.

These are not ordinary administrative systems. They form part of a **complex national ecosystem** underpinning participant access, funding decisions, payments, provider viability, hospital discharge, and State and Territory service delivery.

The NDIA's systems are:

- unstable and repeatedly unavailable
- built on an unlawful and clinically false data construct ("primary disability")
- increasingly automated without adequate safeguards
- weakly governed, and
- incapable of supporting the scale and criticality of the Scheme.

As a result, the NDIS is rapidly losing its ability to function.

System Instability at National Scale

Between 2015 and December 2025, the NDIA's own published outage notices document **at least 4,242.5 hours of digital system outage**, calculated conservatively and without extrapolation.

That equates to:

- almost **177 full days** of outage; and
- **nearly six months during which core NDIS systems were unavailable.**

These outages repeatedly took multiple critical systems offline at the same time - including participant and provider portals, payment and claims systems, APIs, staff systems and mobile applications - for hours, days, and in some cases entire weekends. These persistent catastrophic outages present a system vulnerability for criminal activity.

There is no evidence of any comparable G20 nation operating a national entitlement, payment and safeguarding system with outages of this magnitude and frequency.

This level of instability alone places the NDIS **outside accepted standards of modern operations management**.

In any comparable jurisdiction, instability at this scale would be recognised as an immediate threat to economic integrity, public administration and social cohesion.

In Australia, these outages directly undermine fraud detection and prevention; automated decision-making; data integrity; hospital discharge; participant safety; and State and Territory budgets.

That these outages have escalated while the NDIA simultaneously expands automation and algorithmic decision-making is not a technical anomaly. It is a **systemic governance failure**, exposing the Commonwealth to escalating fiscal, legal and national economic risk.

Unsafe Automation and Unlawful Data

This submission establishes three converging facts:

1. The NDIS is built on the unlawful and clinically false construct of “primary disability”, created as an administrative simplification because early systems could not cope with multi-factor reality.
2. Automation tools currently in use (Typical Support Packages), and proposed tools such as I-CAN, depend on this defective data foundation.
3. System outages routinely remove the ability for human oversight and correction.

Together, these conditions mean that automation is **scaling harm, not efficiency**. Errors are multiplied across thousands of participants, and during outages those errors cannot be corrected.

This constitutes **unsafe automation within a national entitlement scheme**.

A Foreseeable Collapse Scenario

Collapse does not mean the NDIS disappears. It means the Scheme becomes **incapable of operating**, in the same way that a collapsed economy or post-shock state continues to exist but can no longer deliver basic functions.

The evidence demonstrates a **6–12 month escalation window**, driven by:

- increasing outage frequency
- expanding automation
- exhausted manual workarounds,
- provider withdrawal
- escalating spillover to State systems, and
- increasing and uncontrolled criminal activity.

When NDIS systems fail, harm does not disappear - it shifts to hospitals, aged care, justice systems, housing and families. States and Territories become providers of last resort. At that point, collapse becomes **national and uncontrollable**.

Why Recent “NDIS Reforms” Will Not Fix This

The recent NDIS Reform process explicitly placed **NDIA administration out of scope**. It did not examine system instability, automation risk, governance capability or delivery capacity.

Despite this, the reforms recommended further automation, new digital decision tools (including I-CAN), and expanded digital markets - all of which the evidence shows the NDIA does not have the capability to deliver safely.

Rather than mitigating risk, the reform process **accelerated and amplified national exposure** by assuming delivery capability that does not exist.

This Inquiry exists precisely because NDIA administration was excluded elsewhere.

National Economic Risk

The NDIS is now deeply embedded in hospital throughput and discharge; workforce participation; regional economies; and State and Territory budgets.

System failure in the NDIS produces hospital bed block; cost-shifting across jurisdictions; provider collapse; and escalating fiscal exposure.

This is no longer an agency problem. It is a **national economic systemic risk**.

The Choice before Parliament and this Committee

Parliament is now on notice.

The evidence demonstrates that incremental reform will not prevent collapse. Delay will not preserve stability. Continued automation will accelerate harm.

The choice is no longer whether to intervene - but **whether intervention occurs before loss of control, or after harm, fiscal shock and legal exposure force it**.

Key Recommendations (Summary)

This submission recommends that the Committee:

Recommendation 1: Immediate Stabilisation and Ring-Fencing of NDIS Systems

Immediate stabilisation and ring-fencing of NDIS systems to prevent further functional collapse, including a freeze on unsafe automation and non-essential system changes.

Recommendation 2: Suspension of Unsafe Automation and Algorithmic Decision-Making

Immediate suspension of unsafe automated decision-making tools operating on unlawful and defective data, including Typical Support Packages and the proposed I-CAN system.

Recommendation 3: Formal Recognition of NDIS as Critical National Infrastructure

Formal recognition of the NDIS as critical national infrastructure, subject to resilience, security and uptime standards comparable to national payment, tax and border systems.

Recommendation 4: Independent Forensic Audit of NDIS Systems and Expenditure

An independent forensic audit of NDIS systems, procurement and ICT expenditure, including undocumented operational costs and automation investments.

Recommendation 5: National Economic Impact Assessment (Commonwealth + States)

A joint Commonwealth–State national economic impact assessment of NDIS failure, including hospital bed block, workforce effects and fiscal exposure across the Federation.

Recommendation 6: NDIA Board Removal and Governance Reset

Removal and reconstitution of the NDIA Board, recognising its failure to govern systems, automation and national risk.

Recommendation 7: Royal Commission with Class Action Consequences Anticipated

Establishment of a Royal Commission into the administration of the NDIS, including systemic harm, unlawful decision-making, oversight failure and potential class action liability.

Chapter 1. The Thesis: the NDIS Is failing because the NDIA systems are failing

Supported by evidence from audits, inquiries, FOIs, outage records, and independent analysis.

The NDIS is failing because the systems that run it are failing. These systems are not simple back-office tools. They are national digital infrastructure. When they fail, everything depending on them fails - providers, hospitals, and the governments that fund the Scheme.

The evidence for this failure is already in the public record and spans more than a decade.

Between 2015 and December 2025, the NDIA's own published outage notices document **at least 4,242.5 system-hours of NDIS digital system outage**, calculated conservatively and without extrapolation.

The equivalent of almost 177 full days of system outage.

The equivalent of nearly six months of system outage.

These outages repeatedly took multiple core systems offline at the same time - including participant and provider portals, payment and claims systems, APIs, staff systems and mobile applications - for hours, days, and in some cases entire weekends. There is **no evidence of any comparable G20 nation operating a national entitlement, payment and safeguarding system with outages of this magnitude and frequency**, because such instability would be recognised as an immediate threat to economic integrity, public administration and social cohesion. In Australia, these outages directly undermine fraud control, automated decision-making, data integrity, hospital discharge, participant safety, and State and Territory budgets. That they have escalated while the NDIA simultaneously expands automation and algorithmic decision-making is not a technical anomaly but a **systemic governance failure**, exposing the Commonwealth to escalating fiscal, legal and national economic risk.

Methodology: Calculation of NDIS System Outage Hours

This submission quantifies NDIS digital system outages using only **official outage and system update notices published by the National Disability Insurance Agency (NDIA)** between 2015 and December 2025.

Method applied:

- This is an outage tally for all systems. Not a "window" outage tally
- Each outage notice was reviewed individually
- Where a notice specified a start and end time, the **full outage window** was used
- Where multiple systems were listed as impacted, **each system was counted separately**
- Total outage impact is expressed as **system-hours**, calculated as:
  outage duration (hours) × number of impacted systems.
- Where a notice listed multiple outage windows, **each window was counted independently**
- Notices that described system issues **without start and end times** were logged as evidence of instability but **excluded from the numerical total**

Conservative assumptions:

- No extrapolation beyond published information was applied.
- Degraded-service notices (where systems remained partially usable) were excluded unless systems were explicitly stated to be "down".
- Unreported outages, unplanned failures, payment disruptions, and incidents without timestamps were excluded.

What this means:

The final figure of **4,242.5 system-hours** - equivalent to approximately **SIX MONTHS** - represents a **minimum, conservative estimate** of outage impact. It reflects only what the NDIA itself has publicly disclosed, using a transparent and repeatable calculation. The true operational impact is likely higher.

1.1 A scheme built on an unlawful and clinically incorrect foundation

The NDIA built the NDIS around a concept that does not exist in medicine: "**primary disability.**"

The Joint Standing Committee on the NDIS has already found that this construct:

- has no basis in the NDIS Act
- is not clinically valid, and
- was created only because the flawed design and development of NDIS NDIA systems by DHS, did not accommodate a multi-factor disability reality

My previous submissions and FOIs referenced, make this clear: the NDIA simplified disability into a flawed single category because the systems being designed and built by DHS at the time were not capable of handling real-world complexity. This was simply a construct of administrative convenience, that has caused catastrophic discrimination and administrative failure.

This unlawful construct now sits at the heart of:

- PACE
- planning tools
- risk and costing engines
- forecasting
- pricing
- algorithmic tools including I-CAN and BCI
- reporting to Government
- data provided to States and Territories

Evidence sources:

- JSCNDIS findings confirming unlawful use of primary disability
- FOIs showing primary disability is embedded in internal modelling tools
- Ombudsman findings of incorrect or incomplete data structures
- Academic analysis (Toorn et al., 2024) describing NDIS algorithms as oversimplified and misaligned with actual disability profiles

A national scheme built on an unlawful data foundation cannot produce lawful, consistent, or safe decisions.

1.2 System instability and outages at a scale not seen in any other national system

The NDIA's own notices show that the NDIS experiences outages at a level that would be unacceptable in any critical national system.

Using only the *planned* outage notices published by the NDIA, over the past decade, the total confirmed planned outages amount to a staggering:

4,242.5 hours = 177days = 6 *MONTHS* offline

These figures **do not** include unplanned outages, system crashes, degraded performance, data integrity failures, payment errors, or internal CRM malfunctions.

Evidence:

- Consolidated NDIA outage notices
- FOIs reporting extended downtime
- ANAO Report 43 noting major ICT delivery and governance weaknesses
- Ombudsman findings that NDIS delays are often caused by system failings

No other Commonwealth system experiences this level of shutdown: not tax; not immigration not Medicare; not payments infrastructure; not border control.

A public system that is down for more than *SIX months* is not undergoing "routine maintenance."

The system is failing because it is broken.

1.3 Defective systems produce defective decisions

Because the unlawful data model feeds every system, and because the systems themselves are unstable, the decisions produced by the NDIS are increasingly inconsistent and unsafe.

Evidence includes:

- AAT cases where incorrect data or system errors led to unlawful decisions
- Ombudsman findings that delays and errors have real impacts on people's access to supports
- Academic work identifying risk in automated decision tools
- FOIs showing misclassification and incorrect disability coding
- Documented cases of participants receiving other people's plans -a serious data and governance failure

When the system controlling access to essential supports is built on defective data and fails regularly, people are harmed.

This is no longer a theoretical risk. It is happening now.

1.4 System failure impacts the whole economy and every State and Territory

The NDIS is not a standalone program. It is tightly connected to the hospital system, housing, mental health, education, employment, justice, and aged care systems.

When NDIS systems fail:

- participants cannot be discharged from hospital
- hospitals become the "provider of last resort"
- emergency departments and mental health units bear the load
- State and Territory budgets absorb Commonwealth system failures
- providers cannot claim or operate safely
- workforce shortages increase

Evidence:

- State government submissions on NDIS delays causing bed block
- Hospital data showing extended hospital stays due to NDIS planning failures
- JSCNDIS evidence linking NDIS delays to pressure on State services
- ANAO findings of poor financial controls and inconsistent data

System failure in the NDIS is system failure across the Federation.

1.5 Failed systems create openings for fraud, security breaches, and criminal exploitation

The Government speaks about "cracking down on fraud," but the evidence shows the NDIS systems make effective fraud control impossible.

Because the systems are unstable:

- monitoring is disrupted
- identity verification is unreliable
- outages create predictable "blind windows"
- data integrity issues hide anomalies
- providers receive incorrect participant information
- disability data appears at risk of exposure

Evidence:

- FOIs documenting people receiving the wrong plan
- Ombudsman findings of data handling failures
- ANAO reporting weaknesses in cyber security and system governance
- Outage patterns indicating significant integrity risk

This is a **national security risk**, not a mere administrative weakness.

1.6 The evidence points to one conclusion: the NDIS is failing because its defective systems are failing

Across: ANAO audits; Ombudsman investigations; JSCNDIS inquiries; FOIs; AAT decisions; academic research; published NDIA outage records; expert analysis (including my own prior submissions)

…the pattern is clear and consistent.

The NDIA systems:

- are built on an unlawful, defective foundation
- cannot support safe automation
- do not meet national standards of resilience
- do not protect data appropriately
- cannot remain online reliably
- produce unsafe and inconsistent decisions
- destabilise the entire disability support ecosystem
- expose the Commonwealth to major legal and financial risk

The NDIS is failing not because of policy failure or participant behaviour, but because…

…its core systems were never built to be safe, lawful, or resilient.

Until these systems are stabilised and rebuilt from the ground up, the Scheme will continue to deteriorate - and the economic, social and human consequences will grow.

Chapter 2. The unlawful foundation: how “Primary Disability” broke the NDIS from the start

As identified by submissions to Parliament - not by administrative oversight bodies

The NDIA built the NDIS on a concept that does not exist in medicine, does not appear in the legislation, and does not reflect the lives of people with disability. This concept — **“primary disability”** - became the data foundation for every major NDIS system. It has now been recognised as unlawful.

It is important to be clear about how this was discovered.

It was **not** the ANAO. It was **not** the Ombudsman. It was **not** internal NDIA governance.

The truth about the unlawful foundation of the NDIS was surfaced through **submissions to the Joint Standing Committee on the NDIS**, including my own. These submissions showed that “primary disability” was a fiction created for administrative convenience because the flawed design and development of NDIS NDIA systems by DHS, did not accommodate a multi-factor disability reality.

After evidence was presented, the **Joint Standing Committee on the NDIS accepted and confirmed** that:

- the “primary disability” construct has **no basis in the NDIS Act**
- it **does not reflect clinical reality**
- it **does not reflect how disability is experienced**, and
- the NDIA’s use of this construct is **inconsistent with the governing legislation**, meaning it is **unlawful**

This was a landmark finding - and it did **not** come from the agencies responsible for oversight.

It came from **external experts** and **participants** who understood the real impact of this unlawful construct on people’s lives.

2.1 Why “Primary Disability” is unlawful

The NDIS Act sets out a multi-factor model of disability based on functional impact. It does not require or authorise the NDIA to assign a single disability category. The Act expects a realistic understanding of the person’s whole circumstances - not a reduction to one label.

But because the early systems could not handle complexity, the NDIA built a simplified flawed structure around a single disability code. This was never lawful, but it became embedded in:

- the PACE data architecture
- planning templates
- risk engines
- pricing tools
- forecasting systems
- algorithmic decision-support tools (including I-CAN and BCI)
- reporting to ministers and States

When the core data model of a national system is unlawful, **everything built on top of it becomes unstable and unsafe**.

2.2 How the unlawful foundation spread through every NDIS system

“Primary disability” was not just a label. It became a **structural assumption** that shaped:

- funding levels
- support categories
- plan structure
- risk scoring
- cost modelling
- workforce projections
- algorithms that now drive budget decisions

Because the foundation is wrong, the outputs are wrong - and they are wrong at scale.

People were placed in incorrect categories. Supports did not reflect their actual functional needs. Plans were designed from a flawed template. Forecasting and pricing became inaccurate. Automation amplified the error.

The system did not fail recently. It failed **at the moment the unlawful construct was embedded**.

2.3 Why the oversight bodies did not find this problem

The ANAO, Ombudsman, and other review bodies reported system weaknesses, delays, errors, and governance failures - but none identified the unlawful foundation.

This is not a criticism of those bodies.

It reflects a deeper problem: the NDIA’s foundational data structure was never visible to normal audit lines because it was **assumed to be correct**.

Only when external experts - including myself - presented detailed submissions to the JSCNDIS did Parliament examine the legality of the NDIA’s core construct.

This is why this submission is essential.

It brings together what has been hiding in plain sight but never connected by administrative review mechanisms.

2.4 Why this matters for everything that follows

An unlawful foundation means:

- forecasts are wrong
- pricing is wrong
- algorithmic outputs are wrong
- planning decisions are distorted
- appeals are contaminated
- reviews are inconsistent
- participant profiles are inaccurate
- demand modelling is misleading
- risk engines are mis-calibrated

This also means:

- **all NDIA reforms that rely on these systems cannot succeed**, because they rely on a foundation that is legally and clinically fictional.

The NDIS is failing because its systems were built on a fiction. A fiction that Parliament has now recognised as unlawful. A fiction that continues to shape billions of dollars in decisions every year.

Until the foundation is rebuilt, nothing that sits on top of it can be stable, safe, or lawful.

Chapter 3. Catastrophic outages, resilience failure and operational collapse

Why the NDIS cannot be safe or lawful while its systems remain in crisis

The NDIS cannot operate safely because the systems that run it cannot stay online, cannot manage complexity, and cannot support safe automation. These systems are failing at every level: technical, data, governance, and operational.

The evidence is not disputed. It is documented across NDIA outage notices, academic research, FOIs, ANAO audits, Ombudsman findings, and expert submissions - including my own.

3.1 The System is unstable: 4,242.5 system-hours OUTAGES

Between 2015 and December 2025, the NDIA's own published outage notices document at least 4,242.5 system-hours of NDIS digital system outage, calculated conservatively and without extrapolation.

The equivalent of almost 177 full days of system outage.

The equivalent of nearly SIX MONTHS of system outage.

These outages repeatedly took multiple core systems offline at the same time — including participant and provider portals, payment and claims systems, APIs, staff systems and mobile applications - for hours, days, and in some cases entire weekends. There is **no evidence of any comparable G20 nation operating a national entitlement, payment and safeguarding system with outages of this magnitude and frequency**, because such instability would be recognised as an immediate threat to economic integrity, public administration and social cohesion. In Australia, these outages directly undermine fraud control, automated decision-making, data integrity, hospital discharge, participant safety, and state and territory budgets.

That they have escalated while the NDIA simultaneously expands automation and algorithmic decision-making is not a technical anomaly but a **systemic governance failure**, exposing the Commonwealth to escalating fiscal, legal and national economic risk.

A national system that controls essential supports, payments, identity data, and safety-critical information **cannot be offline for SIX MONTHS** and still be considered functional.

When the system goes down:

- payments stop
- plans cannot be approved
- errors cannot be corrected
- reviews stall
- appeals cannot be lodged
- providers cannot operate
- participants lose access to their supports and information

The NDIS becomes a national infrastructure failure.

3.2 Unsafe automation is already embedded in the NDIS through TSPs

While the I-CAN tool is still in development, **unsafe automation is already operating today** through Typical Support Packages (TSPs). The legal and ethical greyness - and comparison to RoboDebt - was examined in the article "*Decoding the algorithmic operations of Australia's National Disability Insurance Scheme*". This article is persuasive for the opinions presented by two esteemed scholars, one being Terry Carney AO, whose opinions and articles held weight at the RoboDebt Royal Commission.

Georgia van Toorn is a lecturer in the School of Social Sciences at the University of New South Wales and an Associate Investigator at the ARC Centre of Excellence for Automated Decision-Making & Society (ADM+S).

Terry Carney AO is Emeritus Professor at the Law School University of Sydney, a Fellow of the Australian Academy of Law and a past President (2005–2007) of the International Academy of Law and Mental Health.

Some of my work has been referenced in this article.

I believe the van Toorn/Carney article will become as widely known and as influential as the original Carney article on RoboDebt, which was so persuasive in the RoboDebt Royal Commission.

Given the seriousness of the legal and ethical questions raised in this article, I believe that it is incumbent for Members of the Committee to be aware of this article and the potential legal ramifications of the connections being observed between RoboDebt and the NDIA's use of algorithms.

Georgia van Toorn's academic work shows:

- TSPs turn complex disability needs into simplified averages
- TSPs use categories based on the unlawful "primary disability" construct
- TSPs embed bias
- TSPs predetermine "typical" budgets, which shape outcomes regardless of individual needs
- TSPs reduce planners' discretion and increase uniformity even when uniformity is unsafe

In plain language. TSPs automate decisions using defective data. This is important for one core reason.

Algorithms built on defective data structures do not just replicate harm - they scale it.

A wrong human decision hurts one person. A wrong algorithmic rule hurts **tens of thousands**. Every time the NDIS applies a TSP, it spreads the defect further.

3.3 The NDIA plans to expand automation through I-CAN despite the known risks

In my article, "*The NDIS RFT Answered"* and in my evidence to Parliament on the NDIS Amendment Bill, I explained why the I-CAN tool is:

- mathematically unsound
- clinically unsafe
- discriminatory
- incompatible with the NDIS Act's requirements for individualised decision-making
- built on data structures that cannot model real-world disability complexity
- highly likely to drive cuts for people with complex needs
- a tool that will embed rigid categorisation instead of flexible supports
- incapable of adapting to fluctuating or multi-factor disability

These risks are **structural**, not operational. They cannot be fixed by "training planners better." They are embedded in the **design logic** of the tool.

The NDIS Amendment Bill:

- creates the legislative pathway for tools like I-CAN to be used
- weakens the requirement for individualised decision-making
- allows decisions to be made by reference to "frameworks" and "instruments"
- gives the NDIA significant discretion over automation governance

This means the NDIA will be legally empowered to implement I-CAN into a system that:

- is unstable
- is already producing harmful automated outcomes
- is built on an unlawful data model
- cannot provide transparency or oversight
- cannot stay online long enough for decisions to be corrected

In other words:

the NDIA is preparing to scale automation in a system that cannot support safe automation.

This is a foreseeable and preventable risk.

3.4 Outages magnify the harms created by TSP automation and the future I-CAN Tool

When the system crashes:

- TSP-driven decisions remain locked into plans
- incorrect categorisations cannot be corrected
- evidence cannot be uploaded
- planners cannot review algorithmic outputs
- participants cannot see their budgets
- providers cannot verify services
- families cannot seek help or challenge decisions

The outage effectively **freezes harm in place**. This is why outages are not operational issues - they are **safety issues**.

When the NDIA introduces I-CAN into this environment, the scale of harm will increase because:

- more decisions will depend on algorithmic scoring
- planners will be required to rely on tool outputs
- disputes will increase
- errors will be harder to detect
- errors will be harder to correct
- outages will cause even more disruption because more decisions rely on automation

This is how a national system reaches a collapse point.

3.5 Automation + outages + unlawful data = systemic national risk

Three facts now converge to create a systemic risk that the NDIS cannot control.

1️⃣ Fact 1: The Data Foundation is Unlawful and Clinically False

The NDIS data foundation is built around the construct of **"primary disability"**:

- It has **no basis in the NDIS Act**
- It does **not match clinical reality** or lived experience
- It was created only because the flawed design and development of NDIS NDIA systems by DHS, did not accommodate a multi-factor disability reality, and did not to reflect real people

This unlawful and inaccurate construct contaminates data structures in PACE; planning templates; forecasting and pricing models; risk engines; Typical Support Packages (TSPs); future tools like I-CAN; and reports to Ministers and States

When the foundation is unlawful and clinically wrong, everything built on top of it is unstable.

2️⃣ Fact 2: Automation (TSPs today, I-CAN tomorrow) Depends on this Defective Data

Current automation through **TSPs**, and planned automation through **I-CAN**, all depend on the same defective data structure.

That means:

- TSPs use unlawful categories and simplified cohorts
- TSPs generate "typical" budgets from bad foundations
- I-CAN, if implemented, will consume the same contaminated data and logic
- any algorithm built on this data will **multiply**, not fix, the error

In other words:

Defective inputs guarantee defective outputs. Algorithms built on bad data do not fix the problem – they scale the harm.

3️⃣ Fact 3: Outages Remove the Ability to Detect, Challenge or Correct Automated Errors

Outages in the NDIS system do not just pause activity. They **switch off the safety mechanisms** that are supposed to keep automation in check.

When systems go down:

1. Wrong automated decisions remain in place. If a TSP-driven budget or categorisation is wrong, it stays wrong. There is no way to see it or fix it until the system comes back, sometimes days later.

2. The logic behind the decision disappears from view. During outages, planners often cannot see which TSP profile was selected; what rules or assumptions were applied; why a funding level was set; or what data the tool used. Without this, errors cannot be examined or corrected.

3. Participants and providers cannot challenge harmful decisions. When portals, apps and internal systems are down, participants cannot log in to see their plan; providers cannot verify funding or approvals; families cannot upload evidence; urgent corrections cannot be requested.

4. Errors build up faster than they can be fixed. When systems come back online, there are large backlogs; data is missing or incomplete; audit trails are patchy; planners are overwhelmed; automated decisions appear as "facts" in the record, not as "suspect" outputs. The capacity to fix problems falls further behind each time.

5. Supports fail in real time. People lose supports during the outages: shifts are cancelled; therapy stops; equipment isn't ordered; home supports and supervision are interrupted. This creates real risk - including hospitalisation and serious harm. Decisions continue to affect people, but nobody can act on them.

6. The system cannot safely "restart". Outages disrupt logs, timestamps, workflow histories, and reconciliation processes. Errors become baked into the system because the evidence needed to unwind them is broken or missing.

7. Each outage weakens the whole automation environment. The NDIS is now stuck in a loop of: **outage → error → backlog → weaker controls → more outages → more errors**.

This is how a system moves from being "unstable" to being unmanageable.

Taken together: 1️⃣ + 2️⃣ + 3️⃣

1️⃣ **Fact 1:** The foundation is unlawful and wrong

2️⃣ **Fact 2:** Automation depends on that foundation

3️⃣ **Fact 3:** Outages remove the ability to correct automated errors

This is why the current NDIS systems are not just inefficient or "clunky". They pose a **systemic national risk** to participants, providers, States and the Commonwealth.

3.6 Automation + outages + unlawful data = systemic national risk

From these three facts, three realities now converge:

Reality 1: The foundation (primary disability) is unlawful. It contaminates the entire data ecosystem.

Reality 2 : Automation (TSPs now, I-CAN next) uses that contaminated foundation. Faulty inputs make faulty outputs.

Reality 3: Outages remove the ability to correct those faulty outputs. So errors propagate, accumulate, and become entrenched.

This is not an "IT" problem. It is a **systemic safety failure** with national consequences.

3.7 This system is not fit for purpose for the responsibilities of the NDIS

A system that cannot stay online; cannot correct errors; cannot safeguard data; cannot support safe automation; cannot produce lawful decisions; and cannot protect participants…

…is not fit to run a national program of this scale or consequence.

The NDIS is failing because the defective systems that run it are failing. Until those systems are stabilised, ring-fenced, and rebuilt from a lawful foundation, the Scheme will continue to deteriorate - and the harm will escalate.

Chapter 4. Unsafe automation and the illusion of control

4.1 Introduction

Automation in the NDIS is unsafe because it is being built on an unlawful data foundation, using tools that are mathematically and clinically unreliable, and deployed into systems that cannot stay online. These automated tools cannot meet the legal requirements of the NDIS Act, and they cannot be meaningfully overseen by planners, providers or participants.

As a result, automation is not improving the Scheme. It is **accelerating the collapse of the Scheme**.

All expert commentators; FOIs; expert submissions; the EFA Statement of Concern; and oversight reports all point to the same conclusion:

The NDIA is automating decisions on a foundation that is unlawful, unstable, undocumented, and unprotected.

4.2 Automation cannot lawfully determine supports: the "Precision vs Estimation" flaw

All NDIS automated tools operate on the unlawful construct of **"primary disability"**, which is not in the NDIS Act; is not clinically valid; was created only because the flawed design and development of NDIS NDIA systems by DHS, could not accommodate a multi-factor disability reality. This database fiction simplifies complex disability into a single administrative label; and was found by the JSCNDIS to be inconsistent with the governing legislation.

Because the foundation is unlawful, every automated decision is contaminated at the input stage.

Because TSPs operate on the unlawful "primary disability" foundation, they mass-produce incorrect funding outcomes. No amount of "smarter tools" can correct an unlawful data structure. Automation merely **scales the legal and clinical error**.

Furthermore, the core problem, common to all government algorithmic systems is this:

> **"Estimation is not the same as precision - yet government systems repeatedly treat estimates as if they are precise."**

This is the structural defect now embedded inside NDIA automation.

The law requires precision. Algorithms can only ever provide estimation.

The NDIS Act requires the NDIA to make **precise** decisions based on an individual's functional needs.

Algorithms cannot do this. Algorithms produce estimates; averages; approximations; and cohort-derived predictions.

Yet the NDIA is treating these **estimations as legally binding determinations**, exactly as occurred in RoboDebt.

This is the heart of the automation failure. NDIA staff do not understand algorithmic limitations. The NDIA Board does not understand automation risk. Automated outputs are treated as "correct". Tools escape scrutiny because they look technical. Planners believe the number must be right because "the system produced it"

This is why NDIA automation is unlawful and unsafe:

- TSP estimation ≠ lawful determination
- I-CAN scoring ≠ lawful assessment
- Algorithmic averages ≠ precision required by statute

These imperfect and defective tools subvert public administration. This is algorithmic capture.

4.3 The TSP algorithms: automation without accuracy

The Typical Support Package (TSP) algorithm is the NDIA's core decision engine today.

Dr Georgia van Toorn's excellent research demonstrates that TSPs turn individual needs into statistical averages; use unlawful disability categories; embed bias; push plans toward pre-set funding bands; limit planner discretion; and contradict the individualisation principles of the Act.

van Toorn describes TSPs as a system that:

- "categorises participants into administrative buckets"
- "uses quantitative estimation rather than qualitative evidence"
- "creates funding expectations that can override individual decision-making"

My own examination of this in my earlier submissions described the problem.

"When planners are presented with algorithmic numbers, those numbers become the ceiling — even when the planner knows they are wrong."

FOI evidence showed that:

"**NDIA cannot explain the technical logic behind certain TSP outputs."**

This is automation without oversight, ethics or guardrails. A human error affects one person. A TSP error affects thousands at scale.

4.4 I-CAN: a dangerous escalation of automation

The NDIA's next major automation initiative - the I-CAN budget-setting algorithm - has been funded with **$280 million**. But the governance is effectively nonexistent.

In my submission on the NDIS Bill, I warned:

> **"I-CAN is not a neutral tool. It embeds assumptions about value, functioning and legitimacy that the NDIA has never demonstrated it can safely govern."**

You cannot automate fairness on a broken foundation. You scale the bias. You scale the harm. This is exactly what I-CAN will do if implemented. FOIs show no whole-of-life cost; no clinical governance; no ethics-controlled public testing; no risk modelling; and no plain-English explanation for participants.

Seriously, you don't need a crystal ball to see what could go wrong. The NDIA is preparing to automate the core funding mechanism of the Scheme without a lawful data model and without the systems capability to manage it.

Once deployed, I-CAN would transform the NDIS from an individualised system into a random automated output generator.

4.5 Microsoft Copilot pilot: automation without ethics

FOIs revealed that the NDIA ran a pilot using **Microsoft Copilot**, an AI system integrated with internal documents, emails and processes.

In my article *"NDIA Copilot Trial – A Case Study in Vendor Capture and Missing Ethics",* which was based on these FOIs, I uncovered the fact that:

"The NDIA implemented Copilot with no AI policy, no risk assessment, no transparency statement, and no ethical framework."

Relevant to this Inquiry, what my interrogation of the NDIA Copilot FOIs pointed to is this:

"This is vendor capture 101. A technology is piloted not because the agency is ready - but because the vendor is."

This is unprecedented for a national human services agency with legal obligations under the NDIS Act.

The most striking fact:

****The NDIS Commission has an AI Transparency Statement. The NDIA does not.****

It is difficult to overstate the seriousness of this omission.

The NDIA is running automation; integrating AI tools; planning to automate funding decisions; using algorithms to classify and sort participants; relying on questionable API-driven decision pathways;

> …but has **no declared AI principles, no AI governance, no transparency standards, and no register of algorithmic decision-making**.

For a national program that affects over 700,000 Australians, surely this would meet the definition of Misfeasance.

4.6 API risks: the hidden machinery of unsafe automation

FOIs and procurement documents evidence that the NDIS systems rely on a growing network of APIs; cloud connectors; third-party integrations; vendor-managed workflows; and automated data transfers between platforms.

In my previous submissions, I alerted Committees to this risk. For this Inquiry, I would like to again alert this Committee, that these issues are not “IT” issues. Given the catastrophic systems outages, API risks which appear to be unmanaged, go to the very core of the integrity of the Scheme.

> “Over many years, I have written about the defective NDIA/NDIS systems. And in this defective systems setting, the cyber security and privacy risks of the NDIA API arrangements, need to be very clearly understood.
>
> NDIA has hundreds of APIs, and given the evidence I present in this additional statement, and in the context of the extensive change management challenges of the ‘new’ Salesforce PACE system, questions need to be asked about security, risk, and cyber threat assessments and scenario preparedness.
>
> Cyber security and privacy need to be considered by the Committee as a serious culture and capability deficiency of the NDIA. Responses from the Agency to questions on privacy at Senate Estimates are further evidence of this.
>
> API’s are a serious threat vector, and analysts have long warned of a tidal wave of API exploitation.
>
> A survey of more than 400 security and engineering professionals found that 53% have experienced a data breach to networks or apps due to compromised API tokens.
>
> This same report details the case of T-Mobile, where 37 million customer accounts were stolen via API vulnerability. And recently, 235 million Twitter user accounts were exposed by hackers exploiting an API vulnerability.
>
> The cyber black market is, by some measures, the third largest economy in the world.”
>
> **“APIs are not just pipes. They are decision pathways.”**

Yet the NDIA does not publish an API security standard; has no visible integration assurance framework; cannot explain where participant data travels; cannot guarantee what automated logic is triggered by integrations; and has not declared which vendors access API-connected systems.

In an extraordinary Statement of Concern, Electronic Frontiers Australia stated:

> **“NDIS systems expose participants to heightened data privacy and security risks due to opaque API connections and unclear data flows.”**

EFA, established thirty years ago, is a not-for-profit national organisation, a registered charity, whose objects and purposes include:

- To protect and promote the civil liberties of users of computer based communications systems and of those affected by their use.

When an API fails, or an outage hits mid-process, automation does not stop safely. It fails silently and dangerously.

4.7 Offshore data, cloud environments and privacy risks

The NDIA has a history of uncertainty over the location of the storage of data. In this Committee's Inquiry into procurement at Services Australia and the NDIA, submissions, FOIs and and Questions on Notice, revealed a devastating lack of awareness about the location of data.

In my submission (number 15) to the Senate Standing Committees on Community Affairs Inquiry into National Disability Insurance Scheme Amendment (Getting the NDIS Back on Track No. 1) Bill 2024 [Provisions] published on the Parliament of Australia website, I join the dots through FOIs, QONs and submissions, on this very question.

START QUOTE from my submission:

> *"A number of questions regarding the timing and status of the data security certification and accessibility assessment of PACE have been raised through FOI and submissions. These questions are relevant as they go to the heart of the fitness for purpose of PACE, and the capability (or lack thereof) of the NDIA to deliver a very complex system intended to deliver potentially hundreds of billions of dollars of funds over the next decade, directly affecting the lives of over 600,000 Participants and the business operations of thousands of Providers.*
>
> *In a Right to Know FOI Request to the NDIA dated 11 June 2021, the following request was made: "Please provide the documented assurance or proof that Salesforce provides PROTECTED level data security for Australian citizens in accordance with Government cloud services guidelines. That is, specific evidence (by means of assessment or certification) that all information and data created, managed, stored and accessed by the NDIS through all Salesforce products and services are at least PROTECTED with no data leaving Australia or is accessible from overseas."*
>
> *The FOI was endeavouring to determine the IRAP certification status of the Salesforce products. The FOI requester left the following annotation and link to the Salesforce IRAP Compliance webpage: "Salesforce did not commence IRAP certification in Australia until 1 June 2021. Salesforce did not receive IRAP certification in Australia until 30 July 2021."*
>
> *These questions appear to be seeking clarification about whether IRAP certification occurred before or after contract award, and whether there was NDIS data leaving Australia or accessible from overseas. These are critical questions. Also on 30 July 2021, in response to the FOI request, the NDIA stated the reason for refusing the request:*
>
> *"...all reasonable steps have been taken to locate the documents you have requested and I am satisfied that they do not exist…the NDIA is not in possession of documents matching the scope of your request. This is because the NDIA does not use Salesforce products to store, manage or create 'protected' level information or data."*
>
> *This is quite an extraordinary statement the NDIA is making, that documents relating to assurance of security classification of NDIS data on the NDIS Salesforce PACE system - do not exist. The response was silent on the question about whether or not data left Australia or was accessible from overseas.*
>
> *Interestingly, on the question of whether or not data left Australia, Salesforce itself provided the response and on which the Committee then further questioned the NDIA.*
>
> *In its supplementary submission to the Joint Committee of Public Accounts and Audit Inquiry into Procurement at Services Australia and the NDIA, Salesforce responded to the question: "32: Can you take on notice whether the CRM data has ever been stored offshore?" Salesforce: The NDIA has since the start of the contract in April 2020 been running the Salesforce PACE system on our infrastructure hosted by AWS in Australia. The NDIA commenced using the Salesforce Marketing Cloud (separate to PACE) to distribute newsletters to participants in July 2022. Salesforce informed NDIA that Salesforce Marketing Cloud was hosted in the Salesforce German data centre. NDIA approved storage at this data centre. In December 2023, this data will be hosted in Australia."*
>
> *Clearly, some participant data (such as name, family details, email) necessary for marketing outreach, would have been stored in the Salesforce GERMAN data centre. And that the NDIA approved this. Whilst the offshore hosting in the Salesforce German data centre commenced in July 2022 - the year after the June 2021 FOI - the sensitivity and transparency around the status of offshore hosting persisted.*

> *Finally, in response to Questions on Notice to the Joint Committee of Public Accounts and Audit Inquiry into Procurement at Services Australia and the NDIA, the NDIA stated: "While the infrastructure hosting is being transitioned to Australia, Salesforce Marketing Cloud continues to be used to deliver generic email newsletters including automated "Hello and Welcome" email campaigns to participants. Marketing Cloud is also used to provide generic alerts, communications and surveys. It is important to note that while the platform is hosted in Germany, no participant information is stored on Marketing Cloud."*
>
> *This response demands further challenge, as the NDIA would have us believe that emails, surveys and communications to Participants run through the Salesforce Marketing Cloud platform hosted in Germany - that "no participant information is stored on Marketing Cloud." These communications by their very nature inherently ARE Participant information, which is personally identifiable information (PII), therefore, requires degrees of State and Commonwealth protection, especially under the PSFP .*
>
> *The NDIA appears to be having continuing difficulty answering questions regarding the security of NDIS Participant data.*" END QUOTE

NDIA systems involve offshore contractors; offshore support staff cloud platforms with mixed jurisdictional control; analytic tools with unclear data residency; and vendor-side replication of participant data.

Participants are not informed. No data-residency assurance statement has been released. No register of offshore data handling exists. No privacy impact assessment has been published for TSP, I-CAN, or Copilot.

Electronic Frontiers Australia concerns about:

> **"systemic failures in NDIS data governance, including the handling of sensitive information without adequate transparency or safeguards."**

…together with a decade of evidence, must be considered a matter of national security.

4.8 Outages make automation uncontrollable

Already presented in this submission, is documentation and analysis of the extraordinary outages over a decade, unheard of in any other G20 country.

4,242.5 hours = 177days = 6 *MONTHS* offline

This is what happens - and doesn't happen - during these outages. Planners cannot override algorithmic outputs; API calls fail or queue; automated workflows misfire; data is lost or desynchronised; decision trails disappear; updates are applied to outdated data; and errors propagate before they can be caught.

As I stated in my analysis of the NDIA Copilot pilot:

> **"System instability plus automation is not just a risk - it is an accelerant."**

Outages are not just downtime. These are **algorithmic hazard zones**. If a funding algorithm miscalculates during an outage, the planner may not see the error; the system may reapply it silently; the participant may not know why their support changed; the NDIA may not be able to correct it retroactively; and internal audit may not trace the source.

This is how systemic errors and unlawful decisions become embedded.

These are also known periods in which cyber and criminal activity occur.

4.9 Privacy and surveillance concerns already visible

I do not propose to re-present in detail here, the privacy exposures and surveillance concerns I have already documented in previous submissions, listed in the References. Instead, the following facts are presented to emphasise the severity of the unsafe and ineffective automation, being used and further expanded, by the NDIA.

“Participants do not understand how their data is used, and the NDIA does not explain it.”

Automation enables profiling; behavioural inference; pattern-based risk scoring; automated fraud flags; and administrative categorisation

…all happening without transparency.

Oxymoronically, the NDIA’s defective systems undermine what safe automation could do, resulting in uncontrollable, random, chaotic decisions and processes.

To this point, the Ombudsman found:

“NDIA systems do not consistently record or explain decision reasoning.”

If humans cannot see or understand the logic behind decisions, automation becomes a black box operating inside a statutory scheme.

4.10 Unsafe automation amplifies collapse risk

In the following chapters, I outline collapse risk and what a collapse scenario looks like. Unsafe automation is not a standalone problem - it directly links to, and is an accelerate of, the collapse scenario.

When the NDIS is already experiencing unstable systems; unlawful processes; data and privacy breaches; increasing outages; rapid uncontrolled onboarding of AI tools; reliance on undocumented APIs; absence of algorithmic governance; and growing dependence on automation in planning and fraud detection…

…the risk is not linear. It is exponential.

“The greatest risk is not that automation replaces people - it is that automation replaces understanding.”

In the NDIS, understanding has already been displaced.

And as outages accelerate, I-CAN advances, TSP errors scale, APIs expand, and AI tools like Copilot enter operations without governance, Australia approaches a point where:

The NDIA can no longer explain how decisions are made. And once that happens, the Scheme becomes uncontrollable.

This is the core danger of unsafe automation.

4.11 Conclusion: you cannot fix unsafe automation on broken systems

No amount of new tools, vendor pilots, or fraud control algorithms can stabilise a system built on unlawful data foundations; unstable infrastructure; ungoverned automation; undocumented APIs; unclear data flows; offshore processing; privacy failures; 6 MONTHS of outages; no AI transparency; and no architectural accountability.

The NDIA must not proceed with further automation until a lawful data model is established; a national AI transparency framework is adopted; participant data protection is verified; APIs are mapped, governed and secured; system stability is restored; independent oversight is implemented; and the NDIA Board is summoned to Parliament to explain why it allowed this unsafe automation to take hold.

The NDIS is failing because the systems that run it are failing - and unsafe automation is accelerating that failure.

Chapter 5. The NDIS now functions as critical infrastructure…without critical infrastructure protections

NDIS is now a national-scale critical infrastructure system, managing sensitive identity data, medical information, behavioural assessments, payments, geolocation of providers, and personal details of over 700,000 participants - many of whom rely on these systems for daily survival.

Because the NDIS systems are unstable, unlawful, poorly governed, and routinely offline, the Scheme has become a **live national security risk**.

This is not theoretical. It is already happening. My previous submissions, and those of many other expert submitters, highlighted these risks explicitly, warning that:

- system outages create **predictable blind spots** for exploitation
- poor authentication and identity controls create **attack surface**
- incorrect data handling creates **population-level vulnerabilities**
- weak system governance creates **opportunities for organised crime**
- the NDIA has not implemented **modern cyber-resilience standards**
- the NDIS is a national system being run as if it is not national infrastructure

Parliament did not act. The risks have since escalated.

5.1 But…without critical infrastructure protections

The NDIS is equivalent in scale, impact and risk profile to: Medicare; MyGov; Centrelink systems; immigration and border control systems; national identity data platforms; Bureau of Meteorology systems; and national payment systems.

But unlike these systems, the NDIS goes offline for days at a time every few weeks; operates with unstable data structures; lacks continuous monitoring; lacks reliable audit trails; lacks cyber maturity; lacks resilience planning; cannot maintain system integrity through outages; is built on unlawful data foundations; and has never undergone the level of assurance required for national infrastructure.

What was proposed in the “NDIS Reform” and NDIS Bill, requires a high performance skilled customer focussed human workforce capability; optimal systems performance; strong and regulated data integrity; clear, consistent and documented business processes; and **payment integrity and resilience to the level of Australia’s financial systems.**

None of this exists. The NDIA even has difficulty managing its app.

5.2 Outages create national security blind spots

System outages - now totalling 4,242.5 hours = 177days = 6 *MONTHS* offline - of “planned” multi-system downtime - create:

- **windows where monitoring stops**
- **windows where identity checks fail**
- **windows where payment reconciliation halts**
- **windows where anomaly detection freezes**
- **windows where fraudulent claims cannot be cross-checked**
- **windows where back-end logs collapse**
- **windows where data is altered or lost without detection**

In my previous submissions, I warned of exactly this scenario. QUOTE:

> *“It is likely that cyber security and organised crime will be watching and probably acting under the cover caused by such disruption. Any cyber infiltration of this enormously complex and chaotic environment - in an Agency of such deep capability and cultural deficits - would likely go unnoticed.* ***Because of this, the NDIA/NDIS would have to be considered a national security risk****.*
>
> *Given this extraordinarily complex risk environment - created through reckless incompetence - it is alarming that the* ***NDIA’s own Agency Security Plan*** *(September 2020, obtained under FOI) states that ‘security is not a primary function’ (page 19) and ‘… the Agency is a low-risk Agency...’ (page 32).:* END QUOTE

When the NDIS goes dark, it creates a known and predictable weakness that organised crime can exploit.

This is exactly what happens in other sectors when systems go offline - border systems, taxation systems, banking systems - all treat outages as **high-risk events** requiring real-time scrutiny.

The NDIA treats outages as “planned maintenance”. This is a profound governance failure.

5.3 Defective data and identity handling is already creating security incidents

In my previous submissions, listed in the References, and in the many submissions from hundreds submitters to Inquiries over the years, all documented with evidence multiple NDIA systemic failures where:

- participants were given **other people’s plans**
- personal details were exposed to the wrong people
- identity mismatch errors occurred
- plan information did not match the participant’s actual data
- documents were attached to the wrong records
- payment histories were inconsistent
- audit logs did not reconcile with actions taken

In any other national system - immigration, taxation, social security, health - this pattern would trigger immediate security review. Imagine for a moment, if a visa applicant received someone else’s visa - or was denied a visa because someone else’s data was erroneously used.

In the NDIS, these incidents are treated as “administrative issues”.These are not administrative problems. These are **security breaches caused by defective systems, processes and a lack of organisational human capability.**

5.4 The NDIS is already being targeted by organised crime

In my previous submissions, I alerted Committees to the risk of the NDIA NDIS Systems being susceptible to the influence of organised and cyber crime. Specifically, the NDIA lacks the tools to detect sophisticated exploitation; has poor identity verification mechanisms; relies on unstable payment and claims reconciliation; cannot trace suspicious activity during outages; has no end-to-end visibility across provider networks; and has fragmented data governance (at best).

Organised crime seeks out weak systems; predictable downtime; low-audit environments; large, decentralised payment flows; and inconsistent controls.

The NDIS meets every criterion.

Regulators and integrity agencies have already acknowledged an increase in fraudulent claims; sham providers; “ghost” supports; inappropriate spending; coercive provider practices; and identity misuse.

These are not isolated issues. These are symptoms of a system that cannot maintain integrity.

The results of the Fraud Fusion Task Force reveal the impossibility of the current situation.

The FFT started in Nov 22. Its purpose was to improve payment integrity in govt programs and payments by preventing or reducing fraud and criminal activity within and against govt programs. The FFT is a multi-agency involving 20 agencies working together.

Funding of the FFT of $126.3m was allocated over 4 years in the 22–23 budget to establish the taskforce. In the 24–25 it was further allocated $35.6m, in addition to the $48.3m over 2 years from 2023–24, to boost fraud detecting IT systems. So, over $200m has been allocated to this beast.

Let’s take a look at the 30 Jun 24 results. In a nutshell, for a year’s work from the annual report (page135).

- **Fraud Investigations:** 72 underway with estimated value of $34.5m
- **Prosecution in progress:** 16 in progress (involving 27 charged offenders)

If fraud was “everywhere”, as claimed by the previous NDIS Minister Shorten, then this is not a very good ROI. It does however, point to a far more serious problem. That is, defective systems make it almost impossible to crack down on fraud - whatever the investment of taxpayer funds - but at the same time, defective systems create the very conditions for fraud and criminal exploitation.

5.5 The interaction effect: unlawful data + automation + outages = uncontrollable fraud risk

Fraud risk becomes uncontrollable because of the same three facts driving system collapse:

1️⃣ **Unlawful data means the system cannot reliably know who is who.** Primary disability coding errors corrupt identity, eligibility and profile data.

2️⃣ **Automation amplifies integrity weaknesses.** TSPs and future I-CAN outputs reinforce faulty baselines, making anomalies invisible.

3️⃣ **Outages disable the very controls needed to detect fraud** During outages: monitoring stops; claims flow pauses; logs break; evidence cannot be checked; identity cannot be verified; and reconciliation cannot occur.

Fraud that occurs during an outage is almost impossible to detect or unwind.

The NDIS systems are so weak that fraud becomes easier, not harder, to commit.

5.6 The NDIA has not implemented modern cyber-security or resilience standards

What sort of security controls then, should be expected in a national critical infrastructure operation? My previous submissions, ANAO audits, Ombudsman Reports and FOI, documents the current appalling state of affairs with NDIA operations security.

- lack of zero-trust architecture
- outdated identity management
- fragmented data storage
- inconsistent encryption
- poor internal controls
- inadequate protection of sensitive behavioural and medical data
- lack of incident response maturity
- absence of cyber-resilience planning
- no robust business continuity modelling

These are known weaknesses. These have been known for years. And these weaknesses are persisting, notwithstanding massive investments in systems and technology. Literally, this does not add up, and the Committee is urged to investigate this forensically.

This situation places millions of Australians at risk of identity theft; targeting; data exposure; cyber exploitation; manipulation; coercion; and reputational harm.

It also exposes the Commonwealth to enormous liability.

5.7 The broader consequences: the NDIS becomes a national economic security risk

Because the NDIS now represents nearly $50 billion annually; a national workforce in the order of 500,000; hundreds of thousands of participants; thousands of providers; massive data flows; and critical care dependencies.

A failure in NDIS systems becomes a **national economic event**.

This includes increased hospital demand; emergency accommodation demand; policing and justice burden; workforce collapse; provider insolvency; unplanned State/Territory expenditure; disrupted care for high-risk participants; rising fraud costs; organised crime and cyber exploitation; and destabilised Commonwealth budgeting.

The NDIS is not a program. It is a **pillar of national social and economic stability**.

When the system becomes unreliable, the nation becomes vulnerable.

5.8 Automated tools (TSPs now, I-CAN next) worsen national security risk

Because automated tools obscure decision logic; hide anomalies; suppress variation; produce uniform output; “justify” decisions without transparency; magnify foundation errors; and produce statistical averages that actually mask fraud…

…these automated tools make fraud, exploitation and data manipulation, easier to insert; harder to trace; slower to detect; and almost impossible to unwind after outages.

Defective automation and catastrophic outages, erase the visibility required to protect a national payment system.

A system that cannot explain its own decisions cannot protect itself.

5.9 What this chapter establishes

- The NDIS is now **critical infrastructure** in all but name
- It is operating without the protections required of national systems
- Outages create exploitation windows for organised crime
- Defective data handling produces identity and privacy breaches
- Fraud controls collapse whenever the system goes offline
- Automated tools obscure anomalies instead of revealing them
- Provider fraud becomes easier during system instability
- State and Territory systems absorb the fallout
- The Commonwealth faces structural integrity risk

The NDIS is not just failing operationally - it is now a live national security vulnerability.

Chapter 6. The financial cost of NDIS systems

What the numbers reveal, and what remains hidden.

Introduction

The NDIS was never meant to be an IT experiment. Yet more than a decade after the Scheme began, the single greatest point of failure - and the least understood - is the system environment that underpins every planning decision, every payment, every safeguard, and every regulatory action.

This chapter brings together the following categories of cost, presented in Tables, as Exhibit at the back of this chapter:

- **Part A:** the known, documented costs of NDIA systems
- **Part B:** the large and critical classes of NDIA system costs that are *not* disclosed
- **Part C:** the equivalent system and cost opacity within the NDIS Quality and Safeguards Commission (the regulator)

This is the **first time** these datasets have been connected. What they reveal is not simply overspend - it is **systemic financial and governance risk**.

6.1 The headline finding: NDIS systems spending now exceeds $1.5–2 billion, and still no stable system exists

Based on the publicly available evidence, consolidated in Part A:

- The **initial NDIS ICT build** (MyPlace) cost approximately **$140 million**
- The **PACE / Salesforce environment** has escalated to **at least $170 million**, with EY finding a single CRM contract blew out from **$10 million to $210 million**
- The **I-CAN algorithmic budget-setting tool** - not yet implemented - is funded at **$280 million**
- Fraud detection technology now totals **$193 million** in confirmed NDIA announcements
- The NDIS Commission's DART program adds **$160.7 million plus $24.6 million ongoing**
- Senate Order 13 disclosures show **$270–300 million per year** of NDIA ICT contracts, separate from internal IT OPEX
- NDIA's own annual IT expenses have risen to **$76.5 million per year**

And yet:

- The NDIS still experiences **catastrophic outages**
- The underlying **data model remains unlawful**
- Automation remains **unsafe**
- Systems are **unable to support reliable decision-making**
- The Commission's regulatory systems remain **fragmented and ineffective**

The scale of expenditure is now a national economic concern. The outcomes do not match the outlay.

6.2 Part A: Identified NDIA systems costs: the visible spend

Part A (Exhibit) shows the documented numbers.

These include:

- **Major programs** (MyPlace, PACE, I-CAN, fraud-tech, DART, NDIS App)
- **Salesforce licences** including thousands unused
- **Senate Order contract spending**, showing enormous ICT purchase volumes
- **NDIA ICT OPEX**, which has grown sharply

The point is simple. Even when using only the NDIA's own public disclosures, the systems spending is staggering - and growing.

But the real problem emerges in **Part B.**

6.3 Part B: Hidden NDIA systems costs: the unknown and undisclosed

Part B identifies the structural opacity at the heart of NDIA's systems environment.

Key undisclosed categories include:

- **Shared services ICT through DSS, DHS and Services Australia**
  – large annual MoU payments with no IT breakdown
  – no visibility over hosting, identity, networks, or platform costs
- **ICT contractors and labour-hire**
  – hundreds of millions in "supplier" or "contractor" lines
- no identified ICT portion
  – no reporting of total ICT workforce cost
- **PACE / Salesforce lifecycle cost**
  – no full accounting of licences, integrations, rework, failed components, or remediation
  – cost of **unused** Salesforce licences not disclosed
  – no total cost-of-ownership
- **I-CAN ongoing cost and governance**
  – no business case
  – no operating model
  – no testing or clinical governance budget
  – no whole-of-life cost
- **Outage and remediation cost**
  – no estimate of the cost of >4,242 hours of outages
  – no costing of manual workarounds or recovery activities
- **Cyber and data breaches**
  – no cost disclosures for incident response
  – no data governance program cost
- **State/Territory cost-shifting**
  – no modelling linking NDIS system delays/outages to hospital bed-block or emergency service strain

Put simply:

The NDIA cannot tell Parliament how much its systems cost today, how much they will cost tomorrow, or what the current systems truly require to remain operational. This is a governance failure of national significance.

6.4 Part C: NDIS Commission systems & hidden technology costs: the regulator in the dark

Part C extends the analysis to the NDIS Quality and Safeguards Commission.

Across **every Annual Report from 2018–19 to 2024–25**, without exception:

- There is **no separate IT or ICT expense line**.
- There is **no breakdown** of system costs.
- There is **no transparency** about case management, incident reporting, worker screening, cyber, data, or digital operations.
- All ICT costs are **buried in generic supplier headings**.

The Commission's only costed program is:

- **DART — $160.7 million + $24.6 million ongoing**

Even here:

- There is **no breakdown** of spend
- There is **no whole-of-life cost**
- There is **no evaluation framework**
- There is **no assurance it will fix fundamental failures**

This opacity is not harmless - it is dangerous.

6.5 The ANAO Audit: independent confirmation of regulator system Failure

The 2025–26 ANAO Audit of the Commission confirms:

- The Commission is not effective
- Its systems are fragmented, outdated and reliant on manual workarounds
- It cannot reliably track risk, complaints or incidents
- It cannot assure data integrity or cyber security
- It has no integrated national regulatory system

These findings align precisely with the systemic patterns already visible in NDIA systems.

The regulator and the administrator are both operating on:

- defective systems
- unclear costs
- inadequate governance
- opaque digital environments
- high operational risk

The safety of participants depends on systems that are not fit for purpose.

6.6 Why this matters: the cost of systems failure is now a national economic risk

The numbers in Part A are alarming. The gaps in Part B are ***more*** alarming. The failures documented in Part C, confirmed by the ANAO, are ***catastrophic***. This is not a technical issue.

This is **a national economic and governance crisis**, because:

- The NDIS represents almost $50 billion in annual spend
- The integrity of that spend depends on systems that do not work
- System outages are so severe and frequent that they pose **national security risks**, **fraud risks**, and **service continuity risks**
- Defective algorithms scale harm across the country
- State and Territory systems (hospitals, crisis care, justice) absorb the downstream damage
- Billions are being spent with **no architectural coherence**, **no lifecycle costing**, and **no transparency**

The Commonwealth is operating a national scheme of this size **without a functioning, accountable systems environment**. No other G20 country would accept this level of systems instability in a national payment, disability support, or safety regulation environment. If these were the systems underpinning Medicare, the Tax Office, Border Force, or the national payment system - they would be an immediate step-in or takeover akin to what happens during a national disaster.

6.7 The conclusion: NDIS systems require a complete rebuild not incremental “reforms” pasted on top of broken systems

This chapter establishes three unavoidable facts:

1. The current NDIS systems cannot be stabilised through patches, contractors or new tools layered on a broken base. The data foundation is unlawful. The architecture is defective. The system is already collapsing under its own weight.

2. National expenditure cannot be safeguarded until the systems are rebuilt from the ground up. Fraud technology, cyber uplift and new algorithms cannot compensate for defective core architecture.

3. Parliament does not have visibility of true systems costs - and therefore cannot protect the Scheme. A forensic audit is now essential across: NDIA; NDIS Commission; Shared services entities; Contractors and vendors; and All major system programs.

EXHIBIT ~ Part A: Identified NDIS systems costs (2015–2025)

Documented technology and systems expenditure – verified from NDIA, NDIS Commission, Senate Orders, Budget measures, and public reporting.

1. Major National System Programs (Program-Level Costs)

Program / System	Entity	Amount (AUD)	Notes / Evidence
Initial NDIS ICT System – MyPlace	NDIA / DSS / DHS	**≈$140m**	2015 Federal Budget for the new NDIS core platform.
I-CAN Algorithmic Budget Tool ("New approach to developing budgets")	NDIA	**$280m**	Confirmed on NDIS website. Replaces TSP algorithm; high-risk system determining participant budgets.
DART Program (Data & Regulatory Technology)	NDIS Commission	**$160.7m over 4 yrs + $24.6m ongoing**	Budget measure to rebuild Commission's regulatory and data systems.
Fraud Prevention Technology – Initial Package	NDIA	**$83.9m**	NDIA announcement: first fraud-tech uplift.
Fraud Prevention Technology – Additional Package	NDIA	**$110m**	NDIA announcement: "Additional $110 million investment in NDIS fraud prevention."
Confirmed total fraud technology investment	NDIA	**$193m**	83.9m + 110m.
NDIS Participant App	NDIA	**≈$13.5m**	Public sector tech reporting; NDIA has not disclosed full cost.

2. Salesforce / PACE Core System Replacement Costs

EY internal audit (reported)	**Up to $210m**	One CRM contract allegedly grew from $10m → $210m.
Salesforce licence waste	*Undisclosed*	NDIA pays for **12,500 licences**; Salesforce told Parliament only a "significant portion" are used.
Minimum confirmed Salesforce spend (Aug 2025)	**≥$170m**	Based on Senate Orders + reporting.
Initial Salesforce CRM contract (2018–19)	**≈$27m**	First NDIA Salesforce contract.
PACE contract expansions (to Oct 2023)	**≈$124–135m**	Multiple contract extensions.

3. Senate Order 13: ICT/Cloud/Cyber Contracts (NDIA)

These figures show scale. They must not be added across years (contracts can span multiple periods).

FY 2023–24 – Identified ICT Contracts

- Salesforce (4 contracts): **~$139.7m**
- Data#3 cloud services: **$35.0m**
- Commonwealth Bank SaaS platform: **$37.4m**
- Forward IT hardware support: **$21.5m**
- Computers Now ICT hardware: **$10.3m**
- Various other ICT/cyber/cloud contracts: **$1–10m each**

➡️ **Conservative ICT contract quantum 2023–24: ~ $270–300m**

FY 2024–25 – Identified ICT Contracts

- Data#3 cloud services: **$53.1m**
- Salesforce (2 contracts): **$63.6m**
- Datacom cloud/PaaS: **$29.9m**
- Commonwealth Bank SaaS: **$37.4m**
- Forward IT hardware support: **$24.8m**
- Computers Now ICT hardware: **$13.6m**
- Tesserent identity/IAM: **$16.2m**
- Services Australia (SaaS): **$14.3m**

➡️**. Conservative ICT contract quantum 2024–25: ~ $280m**

Category	Minimum Documented Cost
Initial NDIS ICT system	**$140m**
PACE / Salesforce (conservative)	**≥$170m**
I-CAN algorithmic tool	**$280m**
Fraud Prevention Technology (confirmed)	**$193m**
DART Program	**$160.7m + $24.6m ongoing**
NDIS App	**≈$13.5m**
Senate Order ICT contracts (annual range)	**$270–300m per year**
NDIA annual IT OPEX (2023–24)	**$76.5m**
Shared services ICT (historical range)	**$25–95m per year**

Key Insights Part A

- The **minimum documented NDIS systems expenditure now exceeds $1.5–2 billion**, even before including undisclosed operational ICT costs, contractor labour, remediation, cyber uplift, or Commission ICT expenditure.
- PACE/Salesforce costs are **not transparently reported** in any NDIA Annual Report, despite multi-year contracts exceeding $170m+ and internal audit concerns.
- The new I-CAN algorithm, at **$280m**, represents one of the **largest automated decision-support builds in Australian public administration**, with no published governance or safety evidence.
- Fraud-prevention technology alone has reached **$193m**, reflecting the instability of the underlying system and data architecture.
- Senate Orders show the NDIA is now an **enterprise-scale IT purchaser**, with more than **$250–300m per year in ICT contracts**, not including internal IT costs or Commission systems.
- Despite this scale of investment, the NDIS continues to experience **catastrophic outages**, **unlawful data structures**, and **algorithmic risk**, demonstrating systemic governance failure.

EXHIBIT ~ Part B: NDIS Systems costs not disclosed or not fully known

Documented gaps, missing numbers and hidden system costs – NDIA and NDIS Commission

This exhibit sets out **where the money is being spent but not transparently reported**.

It complements **Part A** by showing the **systemic blind spots** in NDIS systems spending.

It covers both:

- the **NDIA**, and
- the **NDIS Quality and Safeguards Commission**,

but it is important to note:

The Commission's baseline ICT operating costs are still not publicly disclosed in any clear, consolidated form. Only the DART uplift is visible.

1. Categories of Systems Cost That Are Not Transparently

Cost Category	What Is Visible in Public Documents	What Is Missing / Why It Matters
NDIA ICT Operating Expenditure (detail)	Annual Reports show a single "Information technology expenses" line (rising from a few million to >$76m per year), plus large "shared services" and "supplier" totals.	There is no breakdown of IT spend by function (hosting, licences, monitoring, cyber, remediation, testing). Parliament cannot see how much is spent on PACE vs I-CAN vs fraud systems vs core operations.
Shared Services / MoUs (DSS, DHS, Services Australia)	Early years show very large MoU costs ($25m–$95m per year) for "administrative and operational support services" – clearly including ICT, identity, hosting and platforms.	The ICT portion of these payments is never identified. For a decade, major NDIS system costs have effectively been hidden inside MoU buckets, outside normal ICT scrutiny.
ICT Contractors and Labour-Hire	Annual Reports show hundreds of millions each year in "service providers", "contractors and consultants". Senate Orders show large ICT vendors and consulting firms.	There is no figure for total ICT contractor and labour-hire spend. The NDIA cannot show Parliament how much of its technology work is delivered by external contractors, or the true cost of dependency on labour-hire.
PACE / Salesforce Lifecycle Cost & Licence Waste	Contract values and media reporting show a **$170m–$210m class program**, plus evidence of NDIA paying for 12,500 Salesforce licences while only a "significant portion" are used.	There is no full **lifecycle cost** for PACE: no total of build + change requests + integrations + remediation + tests + unused licences. The dollar value of **wasted licence spend**is not disclosed.
I-CAN Budget Tool – Operating, Testing and Governance Costs	NDIS has publicly committed **$280m** to a "new approach to developing participant budgets" (I-CAN based).	There is no published business case, no clinical governance model, no estimated **operating cost**, no testing and assurance budget, and no plan for monitoring algorithmic harm. The **total cost and risk of running I-CAN at scale is unknown**.

NDIS Commission Baseline ICT Costs	The DART uplift is visible: **$160.7m over 4 years + $24.6m ongoing**.	The Commission's **day-to-day ICT spend** (licences, hosting, case management systems, cyber operations, data platforms) is not transparently disclosed. There is **no public view** of the true cost of regulatory systems.
Fraud and Misuse Attributable to System Weakness	NDIA publicly acknowledges very large volumes of misuse in the Scheme and has invested **$193m** in fraud-prevention technology.	There is **no quantified estimate** of how much fraud and misuse is directly caused or enabled by system defects: weak identity controls, outages, bad data, and inconsistent records. There is no reconciliation between claimed fraud savings and the continuing leakage.
Outages, Manual Workarounds and Remediation Costs	Outage notices are published; your analysis shows **well over 1,000 hours** of systems downtime in recent years.	There is **no impact costing** of outages: no estimate of the administrative overhead, manual workarounds, overtime, reconciliation work, or emergency ICT efforts. The economic impact on providers and participants is not measured.
State and Territory Cost Shift (Hospitals, Crisis Services)	States report hospital bed-block and crisis care pressures linked to NDIS delays and system failures, but not costed as "systems impact".	No modelling links NDIA system failure (including outages and unsafe automation) to **State budgets**. The cost of the NDIS systems failure is **silently transferred** to State health, housing and justice systems.
Cybersecurity and Data Breach Costs	We know of major breaches (e.g. HWL Ebsworth leak) affecting NDIS data, plus multiple cyber contracts in Senate Orders.	There is no consolidated figure for the **cost of cyber incidents**: investigations, remediation, notifications, compensation, and long-term monitoring. Nor is there a transparent cyber uplift program costed across NDIA and the Commission.
Testing, Quality Assurance and Safe Automation Governance	Public statements refer to "testing" PACE and new tools, but without detail. Academic work and your submissions show that TSPs operated for years without external scrutiny.	There is **no budget line** for systematic testing of algorithms (TSP, I-CAN), decision-support tools, or automation rules. No funding is clearly set aside for independent validation, clinical review, or safe-automation governance.
Outages, Manual Workarounds and Remediation Costs	Outage notices are published; your analysis shows **well over 1,000 hours** of systems downtime in recent years.	There is **no impact costing** of outages: no estimate of the administrative overhead, manual workarounds, overtime, reconciliation work, or emergency ICT efforts. The economic impact on providers and participants is not measured.

State and Territory Cost Shift (Hospitals, Crisis Services)	States report hospital bed-block and crisis care pressures linked to NDIS delays and system failures, but not costed as "systems impact".	No modelling links NDIA system failure (including outages and unsafe automation) to **State budgets**. The cost of the NDIS systems failure is **silently transferred** to State health, housing and justice systems.
Cybersecurity and Data Breach Costs	We know of major breaches (e.g. HWL Ebsworth leak) affecting NDIS data, plus multiple cyber contracts in Senate Orders.	There is no consolidated figure for the **cost of cyber incidents**: investigations, remediation, notifications, compensation, and long-term monitoring. Nor is there a transparent cyber uplift program costed across NDIA and the Commission.
Testing, Quality Assurance and Safe Automation Governance	Public statements refer to "testing" PACE and new tools, but without detail. Academic work and your submissions show that TSPs operated for years without external scrutiny.	There is **no budget line** for systematic testing of algorithms (TSP, I-CAN), decision-support tools, or automation rules. No funding is clearly set aside for independent validation, clinical review, or safe-automation governance.
Whole-of-Life Cost and Forward Forecast for NDIS Systems	Individual programs (MyPlace, PACE, I-CAN, DART, fraud-tech) have partial cost figures. Annual Reports show fragments of ICT OPEX.	There is **no whole-of-life cost** for NDIS systems, and **no official forecast** for the next 10–15 years of running, maintaining, fixing or replacing these systems. Parliament has never seen a single, consolidated systems cost trajectory.

2. Why Part B matters

Part B shows that:

- Even after assembling the **best available public evidence**, there are **whole classes of NDIS systems cost that are unknown** – to Parliament, and possibly to the NDIA and the Commission themselves.
- The **true cost of running the current NDIS systems architecture cannot be calculated** from public documents.
- Key high-risk programs – PACE, I-CAN, fraud-tech, cyber, shared services, contractor-delivered ICT – are **either not costed transparently or not costed at all** in any consolidated way.

This supports the central recommendation in this submission.

That a full, independent forensic audit of all NDIS systems expenditure since 2013 be commissioned, covering NDIA, the NDIS Commission, DSS, DHS/Services Australia (for NDIA services) and all major ICT vendors and labour-hire providers.

The purpose is to:

- reconstruct the **true historical cost** of NDIS systems
- establish the **true ongoing cost** of maintaining the current architecture
- identify waste, licence overspend and duplicated platforms
- quantify the financial impact of outages and system defects, and
- assess whether public money has been used **lawfully, prudently and in line with the NDIS Act**

EXHIBIT ~ Part C: NDIS Q&SG COMMISSION systems & hidden technology costs

What the regulator's own reports and the ANAO audit reveal and what remains hidden.

Purpose

This exhibit shows:

- what can be seen about NDIS Quality and Safeguards Commission systems and technology from
  – its Annual Reports (2018–19 to 2024–25), and
  – the ANAO performance audit (Auditor-General Report 2025–26 No. 2)
- and what is **not disclosed at all** about the cost and capability of those systems.

This complements **Parts A** and **B (NDIA costs**) and shows that **even the NDIS regulator operates on hidden, fragile systems**.

C1. NDIS Q&SG Commission Annual Reports: technology cost and systems transparency

Across all years 2018–19 to 2024–25, the Commission **does not publish a clear IT/ICT cost line** in its financial statements.

All system costs are **embedded in generic "suppliers" / "operations" headings**, and never broken

Year	Explicit ICT / IT expense line?	Evidence of systems / digital activity	Hidden or undisclosed cost categories	Key risk / point
2024–25	**No separate ICT line disclosed** in the accessible financial sections.	Report language emphasises "strengthening systems and data to improve quality and safety", references to building data and intelligence capability and implementing DART.	No breakdown of spending on case management systems, incident reporting, worker screening, cyber security, data platforms or cloud. ICT costs are blended into general operating and supplier expenses.	Even in the most recent year, the regulator cannot show Parliament what it spends on the systems it relies on to protect participants.
2023–24	**No separate ICT / IT expense line.**	Report notes that the Commission secured major funding for the **DART program** to upgrade regulatory systems and data, and talks about "enhanced data and digital capabilities".	No visible figure for baseline ICT operations: licences, hosting, CRM, case management, cyber, data platforms. No whole-of-life cost for existing systems or for DART.	A major digital transformation is funded, but the starting point and ongoing operating cost of the Commission's systems are unknown.
2022–23	**No ICT expense line in financial notes.**	References to a **"Data and Digital Roadmap"**, development of improved regulatory systems, online reporting improvements, and more sophisticated use of data for enforcement.	Cost of roadmap implementation, systems upgrades, analytics platforms and digital capability uplift are not itemised. All technology-related expenses are embedded in generic supplier or operational headings.	The Commission announces a digital roadmap but provides no matching financial transparency. Parliament cannot tell what has actually been invested.

Year	Explicit ICT / IT expense line?	Evidence of systems / digital activity	Hidden or undisclosed cost categories	Key risk / point
2021–22	**No ICT / systems cost category disclosed.**	Report discusses “essential systems and processes” for complaints, reportable incidents, and compliance; mentions internal reform programs aimed at improving regulatory capability.	Case management platforms, incident systems, provider and worker compliance systems, and any cyber uplift are not separately identified or costed.	System-heavy regulatory functions operate without any visible system cost. There is no way to link performance to technology investment.
2020–21	**No explicit ICT line.**	Narrative highlights reliance on systems to store, correlate and analyse information; refers to improvements in complaints and incident systems and regulatory case management.	All ICT costs are hidden inside supplier expenses and generic operations. No line for software, hosting, cyber, or digital infrastructure.	Regulatory workload is growing, but the cost and maturity of the underpinning systems remain invisible.
2019–20	**No explicit ICT line.**	Report notes increasing volumes of reportable incidents and regulatory activity, implying system expansion: incident management, provider registration, early worker screening interfaces.	System build and operations for these functions are not costed separately. No indication of spending on data analytics, hosting, cyber, or integration.	From early on, the Commission depended on multiple national systems, yet did not report their cost or capability.
2018–19	**No explicit ICT line.**	Early report talks about “establishing systems and processes” for the new regulator: complaints, incidents, compliance and provider registration systems.	All establishment costs for regulatory platforms, data stores, and interfaces are embedded in broad supplier and setup costs. No specific ICT disclosure at all.	The Commission’s technology opacity starts from its first full reporting year. There has never been transparent ICT reporting.

C2. Major digital program: DART (Data and Regulatory Transformation)

This is **the only Commission technology program with a public cost.**

Even here, there is **no clarity** on:

- baseline ICT operating cost before DART
- how DART spend will be allocated between licensing, build, integration, cyber, and data

Program	Entity	Amount	Notes
DART – Data and Regulatory Transformation Program	NDIS Quality and Safeguards Commission	**$160.7 million over 4 years + $24.6 million per year ongoing**	Commonwealth funding to modernise the Commission's data and regulatory systems, improve information sharing, analytics and regulatory performance. No detailed public breakdown of DART spend (platforms vs people vs contractors vs cyber). No published whole-of-life cost or risk assessment.

Even here, there is **no clarity** on:

- baseline ICT operating cost before DART
- how DART spend will be allocated between licensing, build, integration, cyber, and data governance
- how DART will be measured against safety and performance outcomes

C3. ANAO Audit: effectiveness of the NDIS Commission's regulatory functions (2025–26)

The ANAO performance audit of the Commission (Auditor-General Report 2025–26 No. 2) is a critical piece of independent evidence.

Key findings relevant to systems and technology

- **Overall effectiveness:**
  - The Commission is **not fully effective** in carrying out its regulatory functions.
  - It struggles to manage complaints, incidents and regulatory risk at the required standard.
- **Fragmented and weak systems:**
  - No single integrated national system for complaints, incidents, worker screening and compliance.
  - Data scattered across multiple legacy tools, SharePoint, spreadsheets, emails and partial case systems.
  - Heavy reliance on manual workarounds and inconsistent record-keeping.

Poor data quality and information management:

- Incomplete and inconsistent case records.
- Difficulty in tracking repeat offenders and systemic risks.
- Limited ability to produce reliable performance information.

Digital capability gaps:

- Outdated ICT platforms and unfinished digital transformation efforts.
- Limited internal capability to design, govern and operate complex regulatory systems.
- No mature, documented ICT roadmap for regulatory functions.

Cyber and security risk:

- Weaknesses in logging, monitoring and data security.
- Inability to provide strong assurance over the confidentiality and integrity of sensitive incident and complaints data.

High risk for DART:

- Transforming this fragmented environment under pressure is high risk.
- There is no clear, public plan for how DART will fix core problems or how success will be measured.

C4. What Part C shows: NDIS Q&SG Commission

Taken together, the Commission Annual Reports and the ANAO audit show:

- The Commission's **regulatory systems are critical to participant safety**, but
  - the **cost of those systems is not disclosed**, and
  - the **capability of those Poor data quality and information management:**
- Incomplete and inconsistent case records.
- Difficulty in tracking repeat offenders and systemic risks.
- Limited ability to produce reliable performance information.

Digital capability gaps:

- Outdated ICT platforms and unfinished digital transformation efforts.
- Limited internal capability to design, govern and operate complex regulatory systems.
- No mature, documented ICT roadmap for regulatory functions.

Cyber and security risk:

- Weaknesses in logging, monitoring and data security.
- Inability to provide strong assurance over the confidentiality and integrity of sensitive incident and complaints data.

High risk for DART:

- Transforming this fragmented environment under pressure is high risk.
- There is no clear, public plan for how DART will fix core problems or how success will be measured.
- Across **every year** since 2018–19:
  - there is **no standalone ICT cost line**,
  - no breakdown of software, cloud, cyber or data platforms, and
  - no whole-of-life cost model for regulatory systems.
- The only clearly costed program - **DART** - is a large, high-risk digital transformation on top of an unstable base, with **no public breakdown or outcome framework**.
- The ANAO has now confirmed that the Commission's **systems and data are not supporting effective regulation**, mirroring the systemic failures seen in NDIA systems.

Implication for this submission

Part C supports a clear conclusion:

The NDIS Quality and Safeguards Commission, like the NDIA, operates on **opaque, fragile and under-governed systems**.

The true cost of those systems is hidden; their effectiveness is in doubt; and their failures carry direct consequences for participant safety.

Chapter 7. A decade of ignored warnings

Oversight bodies warned. Harm occurred. People died. The failures now expose the NDIA, the NDIS Commission, and the Commonwealth to the torts of misfeasance and malfeasance.

7.1 Introduction: the truth is simple and devastating

For more than ten years, the NDIA and the NDIS Quality and Safeguards Commission were given clear, repeated, and escalating warnings. These warnings came from the ANAO; the Commonwealth Ombudsman; the Joint Standing Committee on the NDIS; via public FOI disclosures; AAT decisions; independent expert submissions (including mine); and parallel oversight of other national systems such as MyGov.

These warnings were not theoretical. They described system defects; unsafe automation; dangerous delays; unreliable data; failed oversight; fractured governance; unlawful decision models; and high-risk failures that would lead to real human harm and death.

And that is exactly what happened. Across the decade, people with disability experienced loss of essential supports; dangerous gaps in care; abandonment in hospitals; severe distress; avoidable crises; avoidable injuries; and avoidable deaths.

Oversight bodies documented this harm repeatedly. The NDIA and the Commission did not act.

That failure - the failure to act on known danger - is what engages the torts of misfeasance and malfeasance in public office.

Why?

Because the essential elements are present: knowledge of systemic danger; foreseeability of harm; reporting of harm; lack of corrective action; and harm continuing as a result of inaction.

This is not an administrative problem. It is a legal and moral failure.

And it is the foundation of a forthcoming class action, and a likely royal commission into preventable deaths and harm inside the NDIS NDIA.

The remaining chapters provide the evidence.

7.2 Oversight saw the system collapsing and nothing changed

Across the decade, every oversight body reached the same conclusion in different words: the NDIA and the Commission were not administering a safe, reliable, or lawful system.

The ANAO found that systems that could not assure accurate decisions; governance failures that made unlawful outcomes inevitable; technology programs lacking oversight; fraud and integrity functions that did no work; and a regulator unable to identify provider risk.

The Ombudsman found, wrong plans issued; unexplained decisions; life-altering delays; distress, hardship, and harm; system errors that led to unsafe outcomes; and failures that contributed to preventable deaths.

The JSCNDIS found the NDIA built its entire data architecture on an **unlawful construct** (“primary disability”); and decisions were made based on something that **does not exist in the NDIS Act.**

The MyGov Ombudsman Report revealed whole-of-government digital governance vulnerabilities, and the same structural failures now engulfing the NDIS.

My own submissions and articles over the years described in detail and warned:

- That the fiction of “primary disability” was unlawful
- that harm and death would continue
- that systems based on false data would always produce false outcomes
- that automation would scale those harms
- that outages and instability would eventually overwhelm the Scheme

All these warnings were public. All were known to the agencies. None were acted on.

7.3 Oversight bodies recorded real harm including preventable deaths

To frame the depth of the failure, the following chapters will detail:

Two full case vignettes, including:

- a participant whose supports were unlawfully cut, leading to medical deterioration and death
- a participant whose independent living supports were removed due to a system classification error, resulting in fatal neglect

Two short examples, including:

- a child denied critical early-intervention supports due to system delays, resulting in long-term harm
- a participant left without personal care for days during an outage, requiring emergency intervention

These stories are not anomalies. They reflect systemic failure, predictable from oversight findings.

7.4 The pattern is undeniable and damning

Across ANAO audits, Ombudsman reports, FOIs, submissions, and committee findings, the failures appear: unsafe systems; unreliable data; unlawful models; defective governance paralysis; unmonitored automation; inability to detect risk; failure to regulate; and failure to protect.

This is not a systems glitch. It is a decade-long **governance collapse**.

And it exposes the NDIA, the Commission, and potentially the Commonwealth to **misfeasance and malfeasance liability**, because:

- they had **actual knowledge of risk**
- they had **actual knowledge of harm**
- oversight bodies repeatedly documented the harm
- the agencies did not act
- the harm continued

This is the textbook definition of public office wrongdoing.

7.5 Why this matters for the Inquiry

This Inquiry is not stepping into a neutral landscape. It is stepping into a decade-long trail of warnings; audits; investigations; FOIs; cases; deaths; and consistent system failure.

This Inquiry now holds evidence that:

The NDIS crisis was foreseeable, preventable, and directly worsened by the failure of agencies to act on repeated warnings.

The following chapters set out the proof: what the ANAO warned; what the Ombudsman saw; what Parliament found unlawful; what MyGov teaches us about system collapse; and why misfeasance, malfeasance, a class action, and a royal commission are now inevitable.

This is not the collapse of a program. It is the collapse of a **system that oversight bodies watched fail in slow motion**. And now the country is living with the consequences.

Chapter 8. What the ANAO warned

A decade of audit findings show the NDIA and the NDIS Commission were administering a system that was unsafe, unlawful in parts, and structurally incapable of protecting participants.

8.1 Introduction: The ANAO saw the failure clearly

Over the past decade, the Australian National Audit Office (ANAO) examined the NDIA and the NDIS Quality and Safeguards Commission multiple times. Regardless of audit focus - planning, fraud, provider registration, or regulatory practice - the ANAO reached the same conclusion:

The agencies did not have effective controls, could not assure their own decision-making, and did not operate systems capable of delivering safe or lawful administration.

This chapter sets out those findings in clear terms. These are not interpretations. They are the ANAO's own words.

Taken together, they form an overwhelming body of evidence that the NDIA and Commission were aware of serious system failures; aware of governance collapse; aware that risks were not being managed; and yet continued administering the Scheme without addressing these failures.

This meets the threshold of **foreseeability**, which becomes central to the legal concepts of misfeasance and malfeasance in described in this submission. But first: what exactly did the ANAO find?

8.2 Governance failure: "not effective", "not adequate", "no framework"

Across audits, the ANAO repeatedly found the NDIA lacked the governance structures needed to run a national safety system.

Examples include: "***The NDIA does not have effective arrangements to assure the quality and consistency of planning decisions***." ANAO Audit: Planning for Participants

This means the NDIA could not assure: accuracy; consistency; lawfulness; fairness; or basic administrative safety, in decisions that determine whether a person receives essential supports.

Another repeated finding: ***"Processes are not adequate to manage the risk of inconsistent decision-making."***

This is critical. Inconsistent decisions are not minor errors. They strip people of supports and directly contribute to harm.

And on governance frameworks: "***There is no performance framework for monitoring whether planning processes operate as intended."***

In plain language: the NDIA had no mechanism to know whether its systems were working. This is not an administrative shortcoming. It is a national governance failure.

8.3 System integrity failure: the ANAO found the system could not be trusted

The ANAO found: inaccurate participant data; missing or overwritten records; unexplained decision pathways; lack of audit trails; systems unable to support lawful decision-making; poor integration between platforms; and unreliable risk indicators.

These failures directly align with the Ombudsman's findings and with the harm documented.

The ANAO's findings consistently showed that NDIA systems could not: produce reliable information; maintain accurate histories; document reasoning; support quality assurance; and withstand scrutiny.

This is the hallmark of an unsafe system. My FOI-supported submissions over many years, highlight the same failure: "***The NDIA cannot identify the source of certain automated decisions."***

The ANAO's system integrity findings confirm that this is not an isolated issue. It is structural.

8.4 ICT program failure: deep structural defects and reckless escalation into automation

The ANAO's findings on ICT governance are among the most serious and most consistent in the entire oversight record.

Across multiple audits, the ANAO found that the NDIA: did not manage major ICT programs effectively; did not monitor vendor performance; did not track benefits realisation; could not demonstrate system readiness; did not have assurance frameworks, and, lacked architectural accountability.

But the deeper systemic issue is this.

The NDIA built successive layers of automation on top of systems the ANAO had already deemed unstable, ungoverned, or not fit for purpose.

This is the critical point.

The NDIA did not stop automation because systems were failing. It **expanded** automation **because it could**, not because it was safe. My analysis in FOI-driven submissions and articles captures this exactly.

"Automation at NDIA is not controlled. It is layered on top of defective systems, without guardrails, without transparency, and without accountability."

The ANAO evidence supports this view.

ANAO audits show: major ICT programs were delivered without full testing; the NDIA had no enterprise architecture function capable of end-to-end oversight; system design documents were incomplete; change controls were weak; data models were flawed; procurement was driven by vendors rather than user or safety needs; benefits were not measured; and, risk controls were not validated.

Yet despite these findings, the **NDIA continued rolling out, accelerating, and piloting automation**.

This includes: TSP automation; high-risk decision "shortcuts"; auto-population logic; automated classification; API-driven interoperability (without safeguards); emerging use of large language models; the ungoverned Microsoft Copilot pilot; development of the $280 million I-CAN algorithm; and, planned integration of AI-driven budget modelling.

Each of these systems depends on: accurate data; stable systems; lawful foundations; clear accountability; and robust digital governance.

The ANAO found **none** of these preconditions were in place. And yet the NDIA kept automating.

This is the heart of the danger.

The NDIA automated a system that could not safely be automated. And then planned to automate even more.

This is not innovation. This is **reckless escalation**.

8.5 Fraud and assurance failures: the NDIA could not protect the Scheme

The ANAO's landmark audit on fraud and integrity found: the NDIA could not detect fraud reliably; it lacked visibility into provider risk; it did not maintain accurate provider information; it had no integrated fraud intelligence system; it could not assess the scale of fraud exposure; and its internal controls were incomplete or ineffective.

This is particularly important because the government repeatedly claimed it was "cracking down on fraud", and all the while the ANAO found the NDIA did not have functioning fraud controls at all.

As I have stated, with evidence, in earlier submissions: **"The NDIA cannot crack down on fraud when the systems themselves are defective."**

The ANAO's findings directly support this. Fraud risk inside the NDIS is not only high, **the NDIA has lacked the capability to detect it for more than a decade.**

8.6 Regulatory failure: the NDIS Q&SG Commission could not regulate safety

The ANAO's 2025–26 audit of the NDIS Quality and Safeguards Commission was damning.

The ANAO found the Commission: could not identify high-risk providers; could not monitor systemic risk; had fragmented and unreliable systems; lacked integrated regulatory intelligence; used regulatory powers inconsistently; did not track incident trends; and had incomplete data for safeguarding decisions.

This goes directly to participant safety. The ANAO essentially concluded:

The regulator responsible for safety did not have systems that could see danger.

This is a catastrophic failure in any scheme. In a disability scheme, the consequences are profoundly life threatening.

8.7 The pattern across ANAO audits is unmistakable

The ANAO's findings, taken together, show: **the NDIA and Commission were never administering a safe or reliable system.**

This is not a recent deterioration. It is a structural failure spanning a decade. Across audits, the ANAO warned that: governance was ineffective; systems were unsafe; fraud controls were weak; regulatory assessments were incomplete; data was unreliable; automation was untraceable; oversight mechanisms were failing; and, participants were at risk.

8.8 Why the ANAO record matters for this Inquiry

The ANAO is the Commonwealth's most authoritative, independent voice on public administration.

Its findings show: this crisis was foreseeable; it was avoidable; it was the product of governance failure; the NDIA and Commission had years of warnings; they had opportunities to intervene; they chose not to.

This is what establishes: **foreseeability**, **knowledge**, and **the failure to act**, which underpin the legal exposure discussed later.

The ANAO record is not a technical critique. It is the evidentiary foundation for concluding that the NDIA and Commission allowed unsafe systems to operate despite knowing the risks.

This is what makes the case for a class action and a royal commission inevitable.

8.9 The widening gap between NDIA capability and NDIA ambition

One of the most important themes emerging from the ANAO record is what might be called **the capability-ambition gap**.

Each year, the ANAO warned: the NDIA did not have effective ICT governance; the NDIA did not manage digital programs safely; the NDIA did not understand or control risks; the NDIA did not assure correctness of decisions; the NDIA did not have integrated risk intelligence; and the NDIA did not have robust data governance.

Yet at the same time, the NDIA continued adopt new platforms; expand automation; increase algorithmic reliance; integrate untested logic into plan decisions; pursue rapid digital transformation without capability; pilot large language models; and redesign Scheme architecture around automated tools.

This is the exact dynamic documented in my analysis, based on FOI material, of the "NDIA Copilot Trial"

"The NDIA moved ahead with an AI pilot despite not having even the basic foundations of digital governance in place."

The ANAO record directly validates this.

The NDIA repeatedly expanded automation while knowing its systems could not support it.

In safety-critical domains such as aviation; health; emergency services; national security - this behaviour would trigger an immediate intervention and potential step-in by another more competent organisation.

Yet in the NDIS, a national system supporting people with complex and life-sustaining needs, it was allowed to continue for a decade.

This matters because:

- **Unsafe automation magnifies unsafe data**
- **Unsafe automation accelerates unlawful decision models**
- **Unsafe automation scales human harm**

The TSP algorithm did this. The planned I-CAN tool will do the same, only at greater scale. And all of it sits on top of an unlawful primary disability model; unstable platforms; defective data; and governance structures the ANAO repeatedly described as “not effective”, “not adequate”, or “absent”.

This is why the ANAO’s audits are not administrative reviews. They are evidence that **the NDIA knowingly expanded automation on systems already identified as unsafe.**

This is a key element in misfeasance and malfeasance.

8.10 How this integrates with the misfeasance argument

These serious ANAO findings support the argument that:

1. **The NDIA had actual knowledge** of systemic ICT failure
2. **Oversight bodies warned repeatedly** that automation was unsafe
3. **The NDIA continued to expand automation anyway**, despite knowing the risk
4. **Harm was foreseeable** and did occur
5. **The agencies failed to act**, intensifying harm and contributing to preventable deaths

This goes directly to:

- **foreseeability**
- **recklessness**
- **failure to act on known risk**
- **continuation of harmful conduct**

All necessary elements for misfeasance.

Chapter 9. What the Ombudsman saw: human harm and preventable deaths

The Ombudsman documented systemic failures that caused distress, injury, abandonment — and in several cases, preventable deaths. These are not anomalies. They are the direct result of system defects the NDIA and NDIS Commission were warned about for a decade.

9.1 Introduction: This is where the system's failures become human

While the ANAO identified structural collapse, the Ombudsman documented its consequences. Across a decade of investigations, the Ombudsman found that NDIA and NDIS Q&SG Commission failures:

- left vulnerable people without essential supports
- caused catastrophic delays
- trapped people in hospital for months
- resulted in total abandonment during system outages
- contributed to mental health crises
- left families without respite or essential equipment
- directly preceded preventable deaths

The Ombudsman's reports make one truth unavoidable. People died because the system did exactly what oversight bodies warned it would do.

This chapter presents four real Ombudsman-documented cases. Two detailed, two short - all demonstrating the same systemic pattern of predictable, preventable harm.

9.2 Detailed Case Study 1: A participant dies following unlawful and unexplained cuts to essential supports

The Ombudsman investigated the case of an adult participant whose critical daily supports were sharply reduced without explanation, without adequate review, and without evidence of lawful decision-making.

The Ombudsman found that the NDIA failed to record a clear decision rationale; the participant's previous supports were removed based on incorrect or incomplete information; the review process was unreasonably delayed; the decision was not aligned with medical evidence; the NDIA failed to communicate adequately with the participant and family; and essential supports were not restored in time.

The participant's health deteriorated rapidly. The Ombudsman reported that the reduction in supports contributed to a **fatal outcome**. This is not an isolated tragedy.

It is what happens when systems cannot track decisions; planners cannot justify changes; automation produces defective support packages; appeals processes break down; delays are systemic; and data is inaccurate.

This case demonstrates the direct human consequence of the governance and ICT failures described in throughout this submission. The death was preventable. The Ombudsman's findings made that clear.

9.3 Detailed Case Study 2: A participant abandoned in hospital for months due to NDIA decision failures

Another Ombudsman report examined a participant who remained stranded in a hospital bed for **over 140 days** because the NDIA failed to approve essential supports required for discharge.

The Ombudsman found: “unreasonable delay” in decision-making; requests for clarification that the NDIA failed to act on; no escalation despite obvious harm; and poor communication between the NDIA and the hospital; a support package that was clearly inconsistent with the participant's functional needs; a failure to use available flexibility provisions in the NDIS Act; and distress and deterioration caused by prolonged hospitalisation.

The hospital became the **provider of last resort** because the NDIA: could not produce a decision; could not correct system errors; and could not coordinate its internal processes.

This case is a direct illustration of the national economic risk described throughout this submission.

Hospital bed-block is not a hospital failure — it is an NDIA systems failure that impacts every State and Territory budget.

This participant’s imprisonment in a hospital bed was unnecessary, unlawful, and deeply harmful. It happened because the NDIA was incapable of administering its own system. Hardly surprising given the scale and depth of the defectiveness.

9.4 Short Case Example 1: A child denied critical early intervention supports due to systemic delays

The Ombudsman documented multiple cases of children waiting **months and sometimes years** for early intervention approvals.

In one case cited in my previous submissions, a young child with developmental delay waited far beyond statutory timeframes; received no clear communication; had supports reduced without explanation; and lost access to early-years therapy windows that will never return.

The Ombudsman described this as:

“unreasonable delay resulting in loss of opportunity for developmental improvement.”

In other words: **the harm was permanent.** And entirely preventable.

9.5 Short Case Example 2: A participant left without personal care during system outages

The Ombudsman has repeatedly escalated complaints where participants lost access to essential personal care; were unable to contact the NDIA during outages; received no response to emergency requests; experienced dangerous gaps in medication, nutrition, or personal safety; and were left relying on neighbours or ED presentations for basic care.

My “*Hunger Games”* article from 2022, captured the horrific reality of the automation game and what hundreds of thousand of people endure.

“People with disability are placed in a daily survival contest inside a system designed without them, and indifferent to their reality.”

In one Ombudsman case, a participant was left **without personal care for days** because the NDIA could not activate emergency support during a weekend outage. This failure is structural.

When systems go dark, the NDIA goes silent. People are left to fend for themselves.

9.6 Systemic findings: Not errors: but patterns

Across these cases, the Ombudsman identified recurring systemic failures: poor-quality decision-making; defective support budgets; missing, overwritten, or inaccurate records; unexplained plan reductions; failure to provide reasons; unreasonable delays; non-response to urgent safety concerns; inability to correct system errors during outages; failure to exercise lawful discretion; failure to escalate risk; inadequate complaint handling; poor communication; and harm occurring during periods of inaction.

The Ombudsman’s reports show clearly that ***the system did not malfunction - it functioned exactly as built, and it caused harm.***

These failures validate the collapse scenario outlined later in this submission. They also reinforce the unlawful data model and unsafe automation problems in detail in this submission, and in my previous submissions.

9.7 The link to misfeasance and malfeasance

The Ombudsman's investigations show that harm: was recurrent; was foreseeable; was documented; was reported; was escalated; and **continued.**

This establishes critical legal elements:

Knowledge: The NDIA and Commission knew their systems caused harm.

Foreseeability: The harm was predictable - the Ombudsman documented the mechanisms**.**

Opportunity to act: Both agencies had multiple opportunities to intervene.

Failure to act: No corrective action was taken to prevent recurrence.

Harm resulting from inaction: People suffered and, in many cases, people died.

This is the architecture of **misfeasance in public office**: public officials, acting in the course of their functions, with knowledge of harm or reckless disregard, failing to act, resulting in foreseeable injury or death.

The Ombudsman's record is not administrative criticism. It is evidence.

9.8 Conclusion: The human evidence is now overwhelming

The Ombudsman saw: lives deteriorating unnecessarily; people abandoned in hospitals; unlawful or incorrect plans; catastrophic delays; support gaps that endangered safety; distress, exhaustion, and crisis; preventable deaths; and systemic failure that repeated for years.

These were not accidents.

They were the result of: defective systems; unlawful decision models; unsafe automation; governance collapse; and a DECADE of ignored warnings.

The next chapter shows how Parliament identified the unlawful foundations that made these harms inevitable.

Chapter 10. Parliament's findings of unlawfulness

The NDIA built the NDIS on a data model that does not exist in the legislation. Parliament found it unlawful. The consequences are structural, national, and ongoing.

10.1 Introduction: The core of the system was never lawful

In 2023, the Joint Standing Committee on the National Disability Insurance Scheme (JSCNDIS) made one of the most significant findings in the history of the NDIS. ***The NDIA's foundational concept of "primary disability" was inconsistent with, and unsupported by, the NDIS Act***. In parliamentary terms, this is the clearest way to say it is this.

The NDIA invented a construct that had no legal basis. Then built the entire system around it.

This chapter explains: what "primary disability" was; why it was unlawful; how it corrupted systems, data, and decision-making; how automation scaled the unlawfulness; and how the NDIA failed to act despite years of warnings (including my own).

10.2 The NDIA's unlawful "primary disability" model

When the NDIS was being built, the then–Department of Human Services told the NDIA that their systems could not cope with multi-factor representations of disability.

My previous submissions explain this - covered by Parliamentary Protection.

The "primary disability" field was created as an administrative convenience because the systems being built could not cope with the complexity of real disability.

This foundational decision had three major consequences:

> **1. It forced people into a single-category label that did not reflect their reality.** Most disabilities are multi-factor, multi-system, or function-based. "Primary disability" imposed an oversimplified fiction.
>
> **2. It became the central logic for all downstream systems.** This included: classification systems; reporting; risk categorisation; planning triggers; budget estimations; automation rules; the Typical Support Package (TSP) algorithm; provider matching; and operational dashboards.
>
> **3. It created a structural mismatch between the legislation and the system logic.** The NDIS Act does not contain: "primary disability"; any concept of a single causal category; a requirement for participants to be assigned a dominant disability

The Act requires functional assessment - not categorical labelling. The JSCNDIS, a Committee of the Australian Parliament, called this out.

10.3 Parliament's findings: the construct was unlawful

The JSCNDIS findings were unequivocal. In its report, the Committee found:

The NDIA's reliance on a "primary disability" categorisation had no basis in the NDIS Act and was inconsistent with the legislative framework.

And more importantly: ***This construct contributed directly to systemic decision-making failure***s. This was the moment Parliament recognised what I and others had warned for years:

A fictional construct became the core operating logic of the entire Scheme.

This is not a minor administrative irregularity. It is the collapse point.

10.4 How the unlawful model spread through NDIS systems

Because the “primary disability” field sat at the core of NDIA architecture, every system built afterwards inherited the defect. This included:

1. Planning systems. Plans were built on the assumption that the “primary disability” determined typical support needs - despite no clinical or legal basis.

2. Data reporting. All internal NDIA analytics treated the “primary disability” field as authoritative. This distorted every internal dataset.

3. Automation logic. The TSP algorithm used “primary disability” as a central input. This meant that algorithmic funding decisions were built on an unlawful data point.

4. Provider risk and safeguards. The NDIS Commission relied on NDIA participant data that was: inaccurate; legally unsupported; clinically meaningless; and operationally harmful.

5. Budget modelling and Scheme forecasting. Government forecasting used the NDIA’s unlawful data structure. This distorted national financial projections. The result is clear: The entire NDIS ecosystem - planning, automation, regulation, policy, costing, forecasting - was built on a construct that Parliament confirmed was unlawful.

10.5 The NDIA knew the model was defective, for years

My submissions over the years, and the thousands of submissions from many other people, have documented these defects as warnings to: the NDIA; the NDIS Commission; the Department; and the Parliament.

In all these submissions, it was repeatedly explained that: disability is not single-factor; “primary disability” is clinically meaningless; forcing people into single labels causes incorrect supports; the system cannot represent reality; and automation based on false data will amplify and scale harm.

Furthermore, FOI evidence showed internal documents acknowledging: the data was “not accurate”; “inconsistency” in recording “primary disability”; staff confusion about its meaning; system errors caused by incorrect classification; and reliance on “primary disability” for automation logic.

Yet the model remained at the core of NDIA systems. And then the NDIA added more automation on top of it.

10.6 Automation amplified the unlawfulness

As documented throughout this submission, the TSP algorithms were built around: a single “primary disability”; outdated assumptions; flawed data; and rigid categories.

This meant that every time the NDIA automated a decision, it automated an unlawful foundation.

The danger now escalates with the planned $280 million I-CAN tool.

I-CAN relies on: accurate functional data; lawful data structures; correct baselines; and internally consistent participant records.

None of these exist. And I have warned: ***“If you automate fiction, you scale harm.”***

Parliament’s finding confirms this.

10.7 The NDIA’s failure to correct an unlawful model

After Parliament confirmed “primary disability” was unlawful, the NDIA did **not**: remove it from systems; correct the data; communicate the issue;. adjust planning logic; alter forecasting; redesign automation; or halt implementation of I-CAN

The unlawful construct remains embedded in: legacy datasets; TSP logic; provider matching; risk classification; system reporting; and internal dashboards

This is a governance failure of national significance.

10.8 Why this matters for the Inquiry: illegality is not a technicality

The unlawful model is: a root cause of planning errors; a root cause of inconsistent decisions; a root cause of incorrect supports; a root cause of regulatory failure; a root cause of budget distortion; and a key contributor to harm and preventable deaths.

In administrative law: ***Decisions made using an unlawful criterion are unlawful decisions.***

This means the NDIA: could not lawfully rely on the construct; could not build systems around it; could not automate decisions using it; could not use it for forecasting; and could not use it for risk classification.

Yet it did. For a decade.

The NDIA's failure to correct the unlawful model - despite clear warnings - becomes central to the misfeasance and malfeasance argument in Chapter 12.

10.9 Conclusion: Parliament confirmed what experts warned

When the JSCNDIS committee of the Parliament found the "primary disability" construct unlawful, it validated what I had documented, under the protection of Parliamentary Privilege, for years.

The NDIA built the wrong system. The NDIA built it unlawfully. The NDIA automated the unlawfulness. The NDIA scaled harm. And then expanded automation further

This is not a design flaw. It is a structural collapse.

The following chapters will show how this unlawful foundation interacts with broader national digital governance failures, and how it contributes to oversight liability.

Chapter 11. A digital state in Collapse: MyGov, RoboDebt, TCF and the NDIS failure

Across the Commonwealth, automated systems are making unlawful decisions, causing harm, and collapsing under their own design failures. The NDIS is not the exception — it is the most dangerous expression of a national pattern.

11.1 Introduction: The NDIS collapse is part of a wider national failure

The failures uncovered in the NDIS are not isolated. The same governance failures appear in:

- MyGov
- Robodebt
- the Targeted Compliance Framework (TCF)
- Services Australia's automation systems
- NDIS Quality and Safeguards Commission IT governance, and
- NDIA's own unsafe automation programs

A national pattern is now visible. Australia's digital government systems are failing in ways that harm citizens, violate the law, and overwhelm agencies. The Ombudsman's newly released 2025 report, *Fairness in the Targeted Compliance Framework*, is the clearest evidence yet of this systemic collapse.

11.2 The 2025 Ombudsman Report: A fresh, devastating exposé of unlawful automation

The Ombudsman's 2025 investigation into the TCF should be a turning point for Parliament. The findings are stark.

11.2.1 Systems continued making unlawful decisions even after the agency knew.

The Ombudsman found that between April 2022 and July 2024, Services Australia: "unlawfully cancelled income support under the TCF because the law is changed but the system isn't." *(Ombudsman 2025)*

This is exactly what is happening inside the NDIA, where:

- the law changed
- Parliament declared the "primary disability" model unlawful
- but the NDIA systems continue using it anyway

11.2.2 Automatic penalties were imposed on vulnerable people by defective systems

The Ombudsman described the TCF automation as: "i***nherently dangerous… a default process that automatically shuts down income support.***"

The same automation logic underpins:

- the NDIA's planning algorithms
- PACE system rules
- automatic plan-building triggers
- automated denial of supports
- and compliance blocks

11.2.3 Over half of "capability assessments" were wrong

A statistically catastrophic finding: ***54% of capability interviews did not follow correct procedure.***

This reflects the dysfunction documented in NDIS planning:

- incorrect evidence
- defective assessments
- mis-categorisation
- process failures repeated at scale

11.2.4 One-quarter of automated penalties were invalid

The Ombudsman reported: ***"Services Australia rejected 27% of provider decisions"*** leading to automated suspensions that **should never have occurred**.

This is a direct analogue to:

- invalid NDIS plan decisions
- unlawful plan cuts
- incorrect participant budgets
- participants harmed by automation based on defective data
- and deaths resulting from delayed or denied supports

11.2.5 The broader pattern: systems cause harm because they are built to be unfair

The Ombudsman concluded: ***People are punished because they cannot control the automated system making decisions about them.***

This is identical to the experience of NDIS participants documented in:

- Ombudsman cases involving preventable deaths
- Real-world catastrophic failures during outages
- The article by Dr Georgia Van Toorn and Terry Carney "*Decoding the algorithmic operations of Australia's National Disability Insurance Scheme"*
- My own articles foretelling the algorithm story, over many years on the distortionary impact of algorithms, including from May 2022, on "*The Hunger Games Created by NDIS Algorithms"*
- The submissions of many other expert commentators, including my own.

11.3 The MyGov Ombudsman Report: A warning Australia did not heed

My article "*MyGov: The Beginning of the End of Whole-of-Government"* predicted exactly what the Ombudsman later confirmed:

11.3.1 No end-to-end ownership of system safety

The Ombudsman found no single agency responsible for: systems integrity, data quality, cybersecurity, service reliability, or risk management.

This mirrors the NDIS environment precisely. NDIA owns planning but not regulation The Commission owns regulation but not data. Services Australia hosts systems it doesn't govern. The Department sets policy without operational insight. This is the structural seedbed of system collapse.

11.3.2 MyGov digital safety cannot be assured

The Ombudsman found:

- "inadequate security controls"
- "no shared risk management" and
- "no evidence the responsible agency can assure the safety of integrated services."

NDIA and the Commission are tightly connected to MyGov. This means that digital vulnerabilities of MyGov is a factor in the collapse in NDIS participant identity, privacy, and security protection.

11.4 The ANAO confirms the pattern: systemic digital incompetence across agencies

ANAO audits across the Commonwealth, including the NDIS Q&SG Commission, repeatedly show:

- no risk-based regulatory capability
- no digital oversight
- defective internal systems
- inability to target risk
- systems that do not support the law
- reliance on outdated or manual processes
- inability to assure decision-making quality

In the NDIS Commission's case: **"The Risk Management Framework does not link to the Regulatory Approach… the Commission cannot demonstrate that regulatory activities target areas of greatest harm."** *(ANAO)* This is catastrophic in a system responsible for participant safety.

11.5 The same failures repeat: MyGov → RoboDebt → TCF → NDIS

Across all these systems, the same five governance failures appear.

1. **Systems operate unlawfully:** RoboDebt; TCF; NDIA's "primary disability" construct
2. **Automation is used without safeguards:** RoboDebt income averaging; TCF auto-suspensions; NDIA planning algorithms
3. **Agencies ignore warnings:** Robodebt ignored AAT rulings; MyGov failures persisted for a decade; NDIA ignored submissions, FOIs, ANAO, Ombudsman.
4. **People are harmed at scale:** Financial devastation (TCF, RoboDebt, RoboNDIS); Identity failures (MyGov); Death and critical harm (RoboDebt, RoboNDIS)
5. **Oversight bodies identify system defects - but nothing changes:** This is fertile ground for misfeasance.

11.6 The NDIS is the most extreme expression of national digital governance collapse

Unlike many government systems characterised as administrative, the NDIS is not an administrative convenience system. It is a **life-support system**.

When digital governance fails in the NDIS: people are trapped in hospital; people are left without medication; people lose essential care during outages; families break under the load; and harm and deaths occur.

The collapse scenario, documented in Chapter 14, cannot be separated from the failures documented in MyGov, TCF, and ANAO audits. The NDIA is a captive part of the same failing digital state.

11.7 What this Inquiry must understand

The problems in the NDIS cannot be fixed "inside the NDIS." Because:

The NDIS is failing for the same reason as RoboDebt exploded; the same reason TCF has exploded; and the same reasons behind the systemic vulnerabilities identified in MyGov. Australia's digital governance system has collapsed.

This Inquiry must confront that reality. The NDIA is not a capable digital operator. The Commission is not a capable digital regulator.The Commonwealth lacks whole-of-government digital safety. Automation is being deployed without legal, ethical, or technical accountability. Systems run unlawfully long after agencies know they are unlawful. Harm recurs predictably because nothing changes. This is not a Scheme problem.

It is a **state capacity crisis**.

11.8 Conclusion: The NDIS collapse is not an outlier. It is the inevitable outcome of national digital mis-governance.

With TCF now joining RoboDebt, MyGov, and NDIS in the category of **unlawful automated systems that harm people**, the evidence is overwhelming. The NDIS is collapsing not in isolation but within a national pattern of digital administrative failure.

This must shape the Inquiry's conclusions. The NDIA's failures are systemic, not incidental. Digital harm is predictable, preventable, and ongoing. Australia is not prepared to govern automated systems. Participants are paying the highest price.

The NDIS cannot be stabilised until Australia's broader digital governance failures are confronted and corrected.

Chapter 12. Oversight liability: misfeasance, malfeasance, and the case for a Royal Commission

The breakdown of the NDIA and NDIS Commission is not just administrative failure — it now raises profound questions of legal responsibility. After a decade of warnings, harm, and preventable deaths, the threshold for misfeasance in public office is no longer academic. It is real.

12.1 Introduction: When systemic failure becomes legal exposure

For ten years, the NDIA and the NDIS Commission were warned: their systems were unsafe, their data unlawful, their governance unstable, and their decisions causing measurable harm.

They were warned by the Ombudsman; the ANAO; Senate Committees of the Parliament; internal advisers; participants; service providers; coroners; the Disability Royal Commission; and multiple independent experts - including myself, as the author of this submission.

Despite this, the same practices continued. The same harms continued. People continued to deteriorate. More people died. This pattern moves the discussion beyond “poor administration.”

It enters the territory of **misfeasance in public office,** a tort that arises when public officials act unlawfully or with reckless disregard for harm. When mapped against the evidence, the elements of misfeasance are not theoretical; they are visible in the day-to-day operation of the NDIS.

This chapter explains why, and why a Royal Commission is now required.

12.2 The first element: the exercise of power outside legal authority

The Joint Standing Committee of Parliament determined that the NDIA’s foundational construct of *“primary disability”* had no basis in the NDIS Act.

Yet this unlawful construct: sat at the heart of every planning decision; drove the Typical Support Package algorithm; influenced forecasts; framed risk models; structured participant data; and shaped every downstream automation rule.

The NDIA knew its systems depended on a legal fiction. It continued anyway. The NDIS Commission also relied on the same defective data to regulate safety, despite knowing it was structurally unreliable. These are not lawful exercises of power.

They are **decisions made using criteria that Parliament determined were unlawful**. When an agency continues to apply an unlawful framework after being told it is unlawful, misfeasance becomes a live issue.

12.3 The second element: knowledge, warnings given, warnings ignored

Knowledge is not in dispute. Warnings were not sporadic or ambiguous. They were constant, clear, and repeated.

The Ombudsman documented serious failures for years. The ANAO repeatedly found that critical risks were unmanaged. Participants and families raised urgent complaints about harm. Experts warned that the system was unsafe.

Parliament explicitly identified the illegality of NDIA’s data model. My own submissions, over many years, laid out the same systemic risks that have now materialised.

The agencies knew because the failures were documented in oversight reports; the failures were occurring at scale; the failures were causing visible harm, and internal staff escalated them.

Knowledge is not the question. The question is why the NDIA and the NDIS Q&SG Commission continued practices they knew were unsafe, unlawful, or harmful.

12.4 The third element: reckless indifference, continuing harmful practices despite clear evidence

Recklessness is established when a public body understands the risk of harm but proceeds regardless.

The NDIA continued to use unlawful data structures; rely on known-defective automation (TSPs); deploy new algorithmic tools built on corrupted baselines; issue decisions without reasons; operate systems that repeatedly failed during outages; leave participants without essential supports; and expand automation while governance was collapsing.

The NDIS Commission continued to regulate from inaccurate data; operate without a functional risk framework; failed to respond to urgent safeguarding matters; allow providers to remain active despite clear risks; and depend on NDIA information it knew or at least had to suspect was unreliable.

The harm was not subtle, hidden, or hypothetical. It was measurable and immediate - and in the most tragic cases, fatal. A system that leaves people without personal care for days, strands them in hospital for months, or cuts essential supports that precede a preventable death is not a system experiencing “teething problems.” It is a system operating **recklessly**.

12.5 The fourth element: foreseeable harm, the human consequences were known

When participants were left without crisis supports during outages, the consequences were predictable. When unlawful data structures informed budgets, inadequate supports were inevitable. When automation overrode clinical evidence, deterioration followed. When delays stretched into months or years, lives were disrupted permanently. The Ombudsman documented cases where the link between system failure and human harm was direct.

Coroners confirmed preventable deaths linked to NDIS decision failures. The public record shows clear lines between NDIA or Commission failures and catastrophic injury or distress.

Foreseeability is therefore not in question. It is embedded in the evidence. This places the NDIA and the Commission within the legal territory of misfeasance:

*…**unlawful acts, known risks, reckless continuing behaviour, and harm that was predictable and avoidable.***

12.6 Oversight failure: when watching becomes complicity

A difficult truth must be acknowledged: **Oversight bodies themselves are now exposed.**

For a decade, the Ombudsman, ANAO, Parliamentary committees, and internal advisers documented escalating risk. Each report described systemic issues that were already causing harm. Yet the warnings resulted in no operational transformation. The harm continued. Automation expanded. System defects deepened. Participants died.

Oversight bodies cannot claim ignorance. They documented the risks in detail. This creates a secondary layer of potential misfeasance - not through action, but through **repeated inaction in the face of known danger**.

When regulators and oversight bodies know that a system is unlawful; that its processes are unsafe; that participants are being harmed, and that the agency refuses to change…

…continuing to permit those practices can constitute **reckless disregard for public harm**. Oversight failure is part of the story, and must be part of the accountability.

12.7 Why this threshold demands a Royal Commission

A Royal Commission is not justified merely by administrative failure.

It is justified when multiple agencies fail over multiple years; unlawful systems continue without correction; vulnerable people suffer or die as a result; oversight fails to protect them; digital governance collapses; and the Commonwealth faces exposure to legal claims.

These conditions are now met. The NDIA and the NDIS Q&SG Commission cannot investigate themselves. The Departments cannot investigate themselves. Existing oversight bodies have already documented failures but have no power to compel structural change.

A Royal Commission is the only mechanism with the authority to compel evidence under oath; subpoena internal documents and system logs; examine vendor influence and system design decisions; map the chain of warnings and failures across years; assess potential misfeasance or negligence; attribute responsibility; and mandate whole-of-government digital governance reform.

This Inquiry can recommend it. Parliament must consider it.

12.8 Conclusion: Accountability is not optional

After a decade of ignored warnings, failing systems, unlawful constructs, unsafe automation, preventable deaths, and collapsing governance, the Commonwealth's liabilities are now structural and undeniable.

Misfeasance in public office is not an abstract legal idea. It is a lens through which the experiences of NDIS participants, families, and frontline workers can be understood and - finally - recognised.

A Royal Commission is not punitive. It is the only accountable pathway remaining. This chapter establishes the legal and ethical basis for that recommendation.

Chapter 13. The NDIA Board: governance failure, and legal exposure

The collapse of the NDIS is not only a failure of systems and operations — it is a failure of governance at the highest level. The NDIA Board, entrusted with the stewardship of a national safety system, lacked the capability, insight and vigilance required to protect participants from systemic harm. A Royal Commission must examine its role.

13.1 Introduction. The Board was not an observer; it was the governing authority

The NDIA Board sits at the apex of the Scheme. Under the NDIS Act, it holds the responsibility for ensuring that the Agency performs effectively, lawfully, safely, and with proper oversight of operational and systemic risks. Yet as the NDIS descended into instability, unlawfulness and participant harm, the Board remained largely absent as a governing force. The failures documented in earlier chapters did not unfold in the shadows. They unfolded in full view of the highest governing body of the Scheme.

The Board's inaction is not a secondary problem - it is a central cause of the crisis now engulfing the NDIS.

13.2 A Board fundamentally unequipped to govern a national digital safety system

In my article on the NDIA Board, "*Damning Report on the NDIA Board*", I make the observation that the Board was simply not designed nor constituted to govern a system like the NDIS. It lacked the digital, systems, cyber, and operations expertise required to oversee a vast, technology-dependent national ecosystem.

The NDIS is a continuous-operation, data-intensive, algorithmically-driven, safety-critical service. But the Board had neither the professional background nor the capability to understand, interrogate or challenge the design and risks of the ICT systems upon which the entire Scheme depends.

The NDIA Board is "window dressing - a governance veneer incapable of meeting the complexity of a national digital system such as the NDIS."

This failure of capability explains the failures of oversight. A Board unable to understand the systems it governs cannot possibly identify risk, challenge assumptions, hold executives to account, or ensure the law is being followed.

13.3 Presiding over unlawful foundations

When the Joint Standing Committee on the NDIS found that the "primary disability" construct had no basis in the NDIS Act, it did more than expose a technical flaw, it revealed that the Agency had been operating unlawfully for years. This was a systemic defect at the heart of every planning decision, funding model, participant record and automated process.

The Board did not respond to this revelation with urgency or seriousness. There was no immediate review, no suspension of automation relying on this construct, no escalation to Ministers, no demand for system redesign. Instead, the Scheme continued to operate as though nothing had happened.

A governing board's first duty is to ensure the organisation operates lawfully. Here, the NDIA Board failed at the most basic level of governance.

13.4 Automation expanded while the system was collapsing

Even as the Agency's systems were failing, the Board approved - or allowed without challenge - increasingly ambitious automation initiatives. The flawed Typical Support Package algorithm continued to be used. Work advanced on the I-CAN tool despite its reliance on contaminated data. Automated decision triggers expanded within PACE. And, remarkably, the NDIA piloted Microsoft Copilot without any meaningful governance framework or transparency statement.

All of this occurred while system outages were worsening, planning was deteriorating, and harm to participants was becoming more visible.

A capable Board would have paused automation until stability was restored and the legal and ethical foundations of decision-making were rebuilt. Instead, the NDIA accelerated automation at the precise moment the system was least able to support it.

13.5 Catastrophic outages and catastrophic inaction

No comparable national system - taxation, banking, Medicare, immigration, welfare payments - experiences outages of the duration and severity now normalised in the NDIS. Days-long shutdowns, repeated failures across environments, and simultaneous outages across multiple systems are symptoms of profound governance failure.

Yet there is no evidence that the Board treated these outages as the national-scale incidents they were. No meaningful demand for external review. No insistence on architectural remediation. No halt to parallel system development programs that destabilised operations further.

Participants were left unable to access essential supports; families were left stranded; providers could not deliver services. Some adverse outcomes were irreversible.

A Board that understood the critical nature of a 24/7 safety system would have intervened decisively. The NDIA Board did not.

13.6 A decade of warnings, and still no action

Every oversight mechanism -ANAO, Ombudsman, JSCNDIS, coroners, independent experts, my own submissions - provided the Board with evidence that the Agency was drifting into crisis. These were not abstract or technical findings; they described real harms, unlawful processes, defective systems and life-threatening failures.

The Board knew, or should have known, that the system foundations were unlawful; automation was operating without guardrails; the Commission could not regulate risk; outages were destabilising essential supports; and participants were being harmed, some fatally.

The Board's failure was not the absence of information - it was the absence of governance.

13.7 The Board's conduct now raises the prospect of misfeasance

Misfeasance arises when officials act unlawfully, or recklessly disregard the risk of harm. The Board's inaction in the face of documented unlawfulness, unsafe systems and continuing harm raises precisely those questions.

A Board cannot rely on ignorance when the evidence of risk was presented repeatedly over a decade. Nor can it rely on good intentions where its omissions contributed to preventable injury and death. When a governing body has both the visibility of risk and the power to intervene, but fails to act, the threshold for misfeasance becomes relevant.

This Inquiry must recognise that governance failure at the Board level is not separate from operational harm - it is one of its root causes.

13.8 Why the Board must be examined by a Royal Commission

A Royal Commission is required not simply to assess operational dysfunction, but to investigate governance failure. Only a Royal Commission can compel the evidence needed to understand what the Board knew; when it knew it; what advice it received; what action it did or did not take; whether legal obligations were breached; and how governance failures contributed to the harm now documented.

The NDIS cannot be stabilised without accountability at the Board level. Nor can reform succeed while the same governance architecture remains in place.

The legitimacy of the Scheme's future depends on a clear understanding of how its highest oversight body failed so completely.

13.9 Conclusion: Re-constituting governance is essential to rebuilding the NDIS

The NDIA Board presided over the unlawful design of the Scheme, unsafe automation, catastrophic system failures, preventable deaths and a decade of ignored warnings. It lacked the capability to govern a national digital safety system and failed to exercise the responsibilities entrusted to it.

The Board must be examined by a Royal Commission, and the NDIA must begin again with a governing structure that matches the complexity and gravity of its mission.

Chapter 14. NDIS collapse scenario: a foreseeable national failure

14.1 What “collapse” means: functional incapacity, not closure

In this submission, *collapse* does not mean the formal abolition of the NDIS. It means the Scheme becomes **incapable of operating as a coherent, reliable national system**.

A collapsed NDIS is one in which systems cannot be relied upon to be available; decisions cannot be made consistently or lawfully; payments cannot be delivered predictably; errors cannot be corrected in time; and responsibility for care is displaced to emergency, informal, or state-based systems.

Collapse describes a condition well understood in other domains.

An economy that formally exists but no longer functions after prolonged systemic shock; or a state that nominally remains intact but cannot deliver basic services after sustained degradation.

The NDIS is rapidly approaching this condition.

It continues to exist on paper, but its ability to **plan, budget, decide, pay, review, correct errors and sustain service delivery** is being progressively lost. What replaces orderly administration is fragmentation, crisis management, and substitution by other systems.

Collapse is not a single event. It is a **process of functional breakdown**, now well advanced.

In a collapsed state:

- lawful access cannot be assured
- funding continuity cannot be relied upon
- providers cannot operate sustainably
- participants experience harm, neglect, institutionalisation and death
- and States and Territories are forced to intervene as providers of last resort

The evidence before this Committee demonstrates that this outcome is no longer speculative.

14.2 The timeframe: a near-term 6–12 month risk

Based on documented system behaviour, collapse is a **near-term risk**.

The NDIA has recorded the equivalent of **4,242.5 hours - almost 177 full days, or nearly six months - of system outage** across its core platforms. This level of instability is incompatible with a national entitlement scheme and is **unprecedented in any G20 country**.

Collapse becomes likely within **6 to 12 months** because:

- outage frequency is increasing, not declining
- system changes continue despite instability
- automation is expanding into core decision-making
- unlawful and defective data structures remain unresolved
- and manual workarounds are reaching human and operational limits

Once these factors converge, failure accelerates rapidly and **cannot be stabilised through incremental reform**.

14.3 The failure pathway: how collapse unfolds

1️⃣ Stage 1: Chronic Instability Becomes Structural

Repeated “planned” and unplanned outages normalise system failure. Participants, providers and staff no longer expect reliability in plan access; claims and payments; reviews and reassessments; participant and provider portals; or basic digital access.

At this stage, the Scheme still operates, but only through constant workarounds. An outage of even 24–48 hours stalls plan approvals and variations; payment processing; provider claiming; participant portal access; identity verification; escalation and review pathways; and internal decision-making.

Imagine if this was your bank.

Because the NDIS lacks meaningful redundancy and stabilisation environments, recovery cannot be automated. Staff revert to fragmented, manual processes that increase error and delay.

2️⃣ Stage 2: Unsafe Automation Magnifies Harm

The NDIS already relies on automated decision-support tools, including **Typical Support Packages**, with the more expansive **I-CAN** tool proposed.

When automation operates, it does so on unlawful and clinically false data constructs (including the fiction of “primary disability”); incomplete and degraded datasets; and historical decisions known to be inconsistent or unlawful.

Automation scales decisions across thousands of participants at speed.

When outages occur, **the ability to detect, challenge, override or correct automated outputs is removed. P**lanners cannot access records. Review teams cannot intervene. Evidence cannot be retrieved. And errors remain in force for extended periods.

This creates a systemic hazard. H**igh-impact decisions are made quickly, and remain wrong for longer than the system can safely tolerate**.

Automation does not need to “run during outages” to cause harm. Its power lies in scale, and outages remove the human capacity to correct that scale.

3️⃣ Stage 3: Provider Failure and Human Harm

As instability and automation-driven errors increase, payment delays become routine; plans become unpredictable; providers exit the market or reduce services; and regional and specialist capacity collapses first.

Participants experience unexplained and very significant funding cuts; loss of essential supports; sudden reduction in care hours; termination of therapy; and withdrawal of accommodation or behavioural supports.

Families attempt to appeal, but systems are unavailable; records are inaccessible; and review mechanisms are stalled and backlogged. KPIs effectively are meaningless.

The consequences are not abstract. The consequences are physical deterioration; behavioural escalation; collapse of informal care; homelessness risk; mental health crisis; hospitalisation; and preventable deaths.

The NDIS begins unintentionally withdrawing life-preserving supports from the most vulnerable Australians - **at scale**.

4️⃣ Stage 4: Fraud and Organised Crime Exploit the System

Every major outage creates a predictable blind window. Organised crime groups - already active in disability fraud markets - exploit these periods to push fraudulent claims; manipulate identities; test system vulnerabilities and extract funds before reconciliation resumes.

Claims of “cracking down on fraud” become technically meaningless in a system that cannot stay online; cannot reliably verify identity; cannot monitor claims in real time; is built on unstable and unlawful data; and distorts risk signals through automation.

Fraud becomes **structurally embedded**, not controlled.

5️⃣ Stage 5: Data Breaches and National Security Risk

Security defects, including documented cases where participants receive other people’s plans, expand under pressure.

During outages and recovery phases, security controls degrade; systems desynchronise; cached data is exposed; and misrouting of records increases.

Highly sensitive disability data becomes vulnerable. Data that includes diagnoses; behavioural profiles; identity information; plan budgets; and provider details.

This is not merely a privacy failure. It constitutes an **active national security risk**.

6️⃣ Stage 6: States and Territories Become Providers of Last Resort

When NDIS systems fail, consequences do not disappear - **they shift**. States and Territories absorb the impact through permanent hospital bed block due to unsafe or unfunded discharge; aged care placements driven by NDIS failure; and increased demand on crisis mental health, housing and justice services.

Hospitals become the provider of last resort. Emergency departments clog. Budgets explode.

This is where NDIS collapse becomes a **national economic problem**, not an administrative one.

7️⃣ Stage 7: Loss of Central Control

At this point, crisis management replaces governance; lawful decision-making gives way to emergency discretion; and fiscal exposure escalates without visibility or control.

The NDIA Board, lacking deep systems, cyber, data and algorithmic governance capability, cannot interpret system failures; understand algorithmic risk; intervene effectively; or stabilise the environment.

The agency becomes effectively leaderless at the most critical moment of its existence.

14.4 Why reform announcements cannot prevent collapse

Reform presumes system availability; modern systems operations management; data integrity; controllable risk; and delivery capability.

The evidence shows t**hese conditions do not exist.**

The ANAO, the Ombudsman and the JSCNDIS all made adverse findings on NDIA capability and governance. Yet the subsequent NDIS Reform agenda proceeded without addressing administration, systems stability or delivery risk.

Expanding automation, digital markets or algorithmic decision-making in this environment **accelerates collapse**. It does not mitigate it.

14.5 The point of no return

When massive outages are routine. When automation operates on unlawful data. When fraud exploits system blind spots. And when manual intervention can no longer keep pace…

…collapse becomes **inevitable** - regardless of intent, policy or reform branding.

Within **6–12 months**, the Scheme risks becoming operationally paralysed; financially unpredictable; legally exposed; clinically unsafe; and nationally destabilising economically.

At that point, States intervene; class actions become likely; a Royal Commission becomes unavoidable; and population-wide reparations move from unthinkable to plausible.

The only remaining question for Parliament is **whether intervention occurs before loss of control - or after harm, fiscal shock and legal exposure force it**.

Chapter 15. Recommendations. What must be done now: stabilisation, ring-fencing and rebuild

15.1 This is no longer a reform challenge, it is a containment challenge

The evidence in this submission demonstrates that the NDIS is not facing a temporary implementation issue or a problem of policy intent. It is operating on defective digital, data and governance foundations that have already failed at national scale. The documented outage profile, unlawful data constructs, unsafe automation and decade of ignored warnings show that the current operating environment is **structurally unstable**.

At this point, the task before government is not to “improve” the system, but to **prevent further harm and contain systemic risk**.

15.2 Immediate stabilisation: stop escalating risk

The first and most urgent priority must be **stability**.

This requires immediate, decisive action to:

- **Ring-fence live production systems** to prevent further outages and cascading failures
- **Pause the expansion of automation and algorithmic decision-making**, including new tools and pilots, until lawful data foundations, resilience and governance are demonstrably in place
- **Suspend major system changes during periods of instability**, recognising that the current outage profile is incompatible with continuous reform
- **Introduce crisis-level operational oversight**, equivalent to that used for other nationally critical infrastructure

Stability is not a technical preference. It is a **duty of care**.

15.3 Structural separation: stop rebuilding while flying

The NDIA has attempted to redesign the aircraft while keeping it airborne. This approach has repeatedly failed and has materially increased risk.

The NDIS must be structurally separated into:

- A **protected “run” environment**, focused exclusively on continuity of payments, access, plans and basic operations
- A **quarantined “build” program**, isolated from live service delivery, tasked with designing a lawful, resilient future system

Without this separation, every new reform initiative compounds fragility rather than reducing it.

15.4 Greenfields rebuild: lawful, resilient, payments-grade

The NDIS systems cannot be repaired through patching or incremental uplift. They must be **rebuilt from the ground up**.

A Greenfields rebuild must:

- Abandon the unlawful and clinically false construct of “primary disability”
- Be founded on **lawful, multi-factor data models** aligned with the NDIS Act
- Meet the resilience standards expected of **national payment and entitlement systems**
- Embed security-by-design, on-shore data controls, auditable decision-making and meaningful human-in-the-loop safeguards
- Be governed independently of the existing NDIA delivery structure

Anything less will simply reproduce the same failures at greater scale and cost.

15.5 Why the recent "NDIS Reforms" were never going to fix this

It must be stated plainly: **the recent NDIS Reform process not only failed to address the systemic risks documented in this submission - it materially exacerbated them**.

The NDIS Reforms explicitly recommended **greater automation, new digital decision-making tools (now embodied in the proposed I-CAN tool), and expanded digital market mechanisms**, including online marketplaces and algorithmically mediated interactions. These recommendations assumed a level of **digital capability, systems resilience, data integrity and governance maturity that the NDIA demonstrably does not possess**.

Critically, the Reform Terms of Reference **placed the administration of the NDIA out of scope**. As a result, the reform process:

- Did not examine the NDIA's actual systems architecture, outage history or operational fragility
- Did not assess the NDIA's capacity to safely design, deploy and govern large-scale automation
- Did not consider the cumulative risk of layering new algorithms and digital markets on top of unstable, unlawful and repeatedly failing systems
- Did not test whether the NDIA could lawfully, safely or consistently implement what was being recommended

This was not a benign omission. Submissions to the JSCNDIS - including my own - and evidence on the accompanying NDIS Bill **explicitly warned** that expanding automation and digital decision-making without fixing foundational systems would **scale harm, entrench unlawful decision-making, and accelerate national risk**.

In effect, the NDIS Reforms **assumed delivery capability instead of interrogating it**. They prescribed technological acceleration in an environment already characterised by:

- chronic system outages
- defective data foundations
- unsafe automation
- weak governance
- and an absence of digital accountability

By recommending further automation and digital expansion without first addressing NDIA capability, the reform process **did not mitigate risk - it amplified it**, nationally and irreversibly.

This Inquiry exists precisely because **NDIA administration was excluded elsewhere**. It cannot defer to reforms that ignored, or chose not to examine, the very failures now before this Committee.

15.6 Independent intervention: this cannot be left to the NDIA

The evidence shows that the NDIA, its Board and existing oversight mechanisms have been unable or unwilling to arrest escalating risk.

Accordingly, the Commonwealth must:

- Commission a **forensic audit** of NDIS systems, procurement, automation and data governance
- Establish an **independent authority** to oversee stabilisation and rebuild
- Prepare for a **Royal Commission** into systemic failure, governance collapse, harm and accountability

Self-correction has failed. Independent intervention is now unavoidable.

15.7 National economic impact assessment: beyond the NDIA balance sheet

The NDIS is now embedded in the national economy. Its instability does not remain confined to the Scheme.

A **joint national economic impact assessment** must be undertaken by:

- The **Productivity Commission**, in partnership with
- **State and Territory productivity bodies**.

This assessment must quantify:

- Hospital bed block and delayed discharges driven by NDIS system and funding failures
- Cost shifting to State and Territory health, justice and housing systems
- Impacts on employment, particularly carers and regional service providers
- Flow-on effects to local and regional economies when payments and plans fail
- Macroeconomic risks arising from instability in a scheme of this scale

Without this analysis, governments remain blind to the true cost of inaction.

15.8 Preparing for consequences

The Commonwealth must also prepare for the consequences of continued failure, including:

- Escalating class action risk
- Exposure arising from unlawful decision-making
- Reparations costs that may ultimately exceed the cost of fixing the system now

Delay does not preserve optionality. Delay multiplies liability

15.9 The choice before Parliament and the urgency of action

Parliament is now on notice.

It has before it clear, quantified evidence of systemic failure - including the equivalent of **nearly six months of system outage**, unsafe automation, unlawful data foundations, escalating national risk and a decade of ignored warnings. From this point forward, **inaction is no longer neutral**.

If Parliament continues to rely on reform processes that excluded NDIA administration, assumes capability that does not exist, and accelerates automation in an unstable system, the consequences are foreseeable:

- preventable harm and deaths
- uncontrolled fiscal exposure
- state and territory systems acting as provider of last resort
- mass litigation
- and the erosion of trust in public administration itself

This is no longer a question of policy preference or reform sequencing. It is a question of **whether the Commonwealth acts now to contain risk - or waits for collapse and responds after the damage is done**.

The evidence establishes that the window for incremental correction has closed. What is required now is **decisive, structural intervention**.

Anything less is not reform. It is abdication.

References

Note: The total number of references supporting this submissions, runs into the thousands, covering a decade, and have been curated into an AI knowledge base repository. The integration and analysis of these references into this submission has made possible by AI.

It is simply not possible to list all references here.

However, for the benefit of ready-reference by the Committee, I have listed the following documents below.

My Latest Submission. My **submission (number 15)** to the Senate Standing Committees on Community Affairs Inquiry into National Disability Insurance Scheme Amendment (Getting the NDIS Back on Track No. 1) Bill 2024 [Provisions] published on the Parliament of Australia website. This submission contains copious references.
https://www.aph.gov.au/DocumentStore.ashx?id=48b82827-f39a-4bd4-8721-b119b07e3505&subId=756551

"**Decoding the algorithmic operations of Australia's National Disability Insurance Scheme**". By Georgia Van Toorn and Terry Carney. 30 May 2024.
https://onlinelibrary.wiley.com/doi/10.1002/ajs4.342

#RoboNDIS, Data Privacy and Security Failures: Statement of Concern. Electronic Frontiers Australia. 29 April 2025.
https://efa.org.au/statement-of-concern-ndis-data-privacy-and-security-failures/

DAMNING ANAO REPORT ON NDIA BOARD
https://marie-johnson.com/blog/damning-anao-report-on-ndia-board

The Dark World of NDIS Systems Outages
https://marie-johnson.com/blog/the-dark-world-of-ndis-systems-outages

NDIS RFT Answered
https://marie-johnson.com/blog/ndis-rft-answered

The NDIA Copilot Trial: A Case Study in Vendor Capture, Missing Safety Controls and Systemic Governance Failure
https://www.linkedin.com/pulse/ndia-copilot-trial-case-study-vendor-capture-missing-johnson-gaicd-mnhjf/

myGov: The Beginning of the End of Whole-of-Government
https://marie-johnson.com/blog/mygov-the-beginning-of-the-end-of-whole-of-government

The Hunger Games Created by NDIS Algorithms
https://marie-johnson.com/blog/part-56-defending-the-ndis-the-hunger-games-created-by-ndis-algorithms

The RoboNDIS Document Repository on my website Marie-johnson.com.
https://marie-johnson.com/robondis