Zen Dodd
POLICY AND PUBLIC SUBMISSIONS

04 NOV 2026

Submission to the inquiry into Australia’s national civil preparedness and resilience

Parliamentary Joint Committee on Defence - Australia

steadytao.com/s/83da859c

Executive Summary

Australia cannot support national defence if the civilian systems which sustain government, communities, industry and the Australian Defence Force stop working when normal suppliers, networks or support arrangements fail.

Australia already has substantial preparedness machinery. The 2026 National Defence Strategy places national civil preparedness and resilience within National Defence. The Australian Government Crisis Management Framework provides national coordination, the Australian Disaster Preparedness Framework identifies 21 national capabilities and the Security of Critical Infrastructure regime requires covered entities to manage material risks. The enhanced critical infrastructure risk management program introduced on 10 June 2026 materially strengthened that regime for specified communications, energy, freight and water assets.[1] [2] [3] [4]

The public record does not yet establish one national account of which civilian functions must continue, what minimum service each must provide, which dependencies are shared across sectors, who resolves competing priorities or what evidence proves that recovery is possible. Protected arrangements may answer parts of those questions. The Committee should determine what already exists before recommending another body or reporting system.

Preparedness should begin with functions rather than regulated asset classes. Emergency calling, public warning, government decision-making, electricity distribution, water, payments, food, medicines, transport and communications each need a minimum service, accountable owner, dependency picture, degraded operating mode and tested recovery path. A second supplier is not independent when both depend on the same cloud, carrier, identity provider, software component, fuel depot or specialist workforce. A backup is not recovery until restoration has succeeded.

Digital continuity deserves specific attention because almost every physical service now depends on software, communications, identity, timing, positioning, data and remote support. Australian Signals Directorate (ASD) CI Fortify guidance already asks critical-infrastructure operators to prove that vital operational technology can remain isolated for three months while critical services continue and can be rebuilt completely. Australia should apply the same outcome-based discipline to every high-consequence digital system while selecting the endurance period according to the function and threat.[5]

National cyber coordination should also be reviewed against the Forum of Incident Response and Security Teams (FIRST) Computer Security Incident Response Team (CSIRT) Services Framework. Relevant teams should have clear mandates and constituencies plus known services for event management, incident management, vulnerability management, situational awareness and knowledge transfer. FIRST supplies a useful service language. It does not establish Australian authority, non-cyber continuity, capacity or maturity.[6]

This submission recommends a permanent cycle through existing institutions: define essential functions, map shared dependencies, set measurable outcomes, exercise realistic failure, correct what fails, retest and report. Emergency authority and protected dependency information need exact legal and access controls. Public reporting should show whether capability exists without publishing an attack guide.

1. Introduction

I make this submission in my personal capacity. I work with software, infrastructure and security evidence so my focus is how Australia's essential civilian functions would operate and recover when ordinary technical and commercial assumptions no longer hold.

The inquiry's five terms are inseparable. Continuity of government and essential services depends on cooperation across jurisdictions. Most critical infrastructure is privately operated. Logistics, manufacturing, resources and primary industries depend on smaller suppliers and skilled workers. Communities include the people who operate services, provide local knowledge and need support when standard channels fail. International partners provide technology, intelligence, transport, supply and mutual assistance. A weakness in one relationship can disable the others.[7]

Civil preparedness should cover conflict, coercion, sabotage, cyber attack, natural hazard, technical failure, supply interruption and combinations of those conditions. A dependency can fail through hostile action, commercial collapse, an unsafe update, a lawful foreign restriction or ordinary engineering error. National arrangements should therefore test consequences rather than assume that one cause or portfolio will own the complete event.

National resilience is also different from ordinary organisational continuity. Several entities may each have a reasonable recovery plan while competing for the same telecommunications, fuel, transport, cloud capacity or specialist labour. One

organisation can meet its recovery objective by consuming capacity required by a more consequential national function. The Commonwealth needs an accountable process for aggregate capacity, priority and deconfliction.

The existing frameworks should be connected rather than replaced. The Australian Government Crisis Management Framework is the capstone for near-term preparedness, response, relief and early recovery. It does not address prevention, long-term reconstruction or risk reduction.[8] The Office of Supply Chain Resilience already assesses vulnerability, criticality, residual risk and proportionate policy responses for essential goods and services.[9] The missing public evidence concerns how strategic intent, regulated assets, shared dependencies and tested recovery are joined across the complete national system.

2. Essential functions and shared dependencies

An essential function is an outcome needed to sustain constitutional government, life, safety, civil society, economic exchange or support to Defence. This is more useful than treating a sector name as the unit of preparedness. "Telecommunications" does not explain the different requirements for emergency calling, public warning, government priority communication, consumer voice, mobile data, satellite access or inter-carrier routing. "Health" does not separate emergency care, medicines, pathology, patient identification, blood supply and public-health coordination.

Each vital function should have a controlled continuity record. It should identify the accountable Commonwealth owner and participating jurisdictions, the people and places served, the minimum acceptable service, maximum tolerable interruption, priority rules, degraded operating mode, dependencies, alternate arrangements, recovery order and supporting evidence. It should also identify unresolved deficiencies, the person responsible for correcting them and whether the correction has been retested.

The records should expose dependencies which cross conventional sectors. A hospital, fuel distributor, supermarket, port and emergency service may all rely on the same mobile carrier, cloud region, identity provider, payment network, positioning service or software-update channel. Infrastructure Australia has previously found that cross-sector interdependencies are often poorly understood and that inconsistent risk methods limit shared understanding.[10]

A national dependency picture should identify concentration, substitutability, endurance and restoration conflicts. It should include energy, fuel, water, transport, communications, satellite links, domain-name resolution, routing, public-key infrastructure, trusted time, positioning, cloud, identity, payments, software, firmware, update channels, hardware, spares, licences, foreign legal restrictions and people. It should test common modes of failure. Two data centres do not provide diversity if they share power, fibre, administration or control software. A local copy is not a recovery capability if it cannot start without a remote licence service.

This does not justify indiscriminate localisation. The Productivity Commission's supply-chain work provides a better discipline: identify vulnerability, criticality and residual risk then select a proportionate response. International diversity, substitution, contingent contracts, stock and domestic repair may provide better resilience than local production in a concentrated market.[9]

The national picture should be protected and federated. Lawful owners should retain operational detail while common identifiers and controlled queries reveal shared dependencies. Access should be purpose-bound, logged and independently reviewed. Parliament and the public should receive aggregate findings, responsible owners, evidence classes and overdue corrections without exact configurations, vulnerable sites or response credentials.

The Department of the Prime Minister and Cabinet (PM&C) should own the whole-of-government strategy and annual account. Defence should state the civilian support it requires. Home Affairs should coordinate civil capability assessment with the National Emergency Management Agency (NEMA) responsible for its emergency-management and community functions. ASD and the Cyber and Infrastructure Security Centre (CISC) should retain their established cyber and critical-infrastructure roles. Sector departments, regulators and jurisdictions should remain responsible for functions within their authority.

3. Digital continuity and critical infrastructure

The Security of Critical Infrastructure regime already requires covered entities to consider cyber, physical, personnel and supply-chain hazards. Australia materially expanded that regime on 10 June 2026. Enhanced CIRMP requirements now apply to specified broadcasting, domain-name, electricity, energy-market, freight, gas, liquid-fuel and water assets. The amended Rules add explicit credential-compromise and lateral-movement hazards plus enhanced cyber, personnel, supply-chain, physical and

natural-hazard requirements. Critical telecommunications assets remain under the separate Telecommunications Security and Risk Management Program (TSRMP).[4]

Those obligations are substantial and should not be duplicated. They remain asset and entity focused. They do not by themselves establish whether dependencies shared across sectors have been identified, whether aggregate capacity is adequate or who resolves conflicting recovery priorities. A national continuity process should consume CIRMP and TSRMP evidence then address only residual gaps.

CI Fortify provides the clearest existing outcome. Operators should identify vital operational technology and enabling systems, prove that they can maintain critical services while physically isolated for three months and prove that they can rebuild those systems completely.[5] The exact period will not suit every function but the form of the requirement is correct: a tested operating and restoration outcome rather than possession of a plan.

Current Commonwealth evidence shows why the distinction matters. In 2025, 82% of Australian Government entities reported having a cyber security strategy but only 22% reached Essential Eight Maturity Level 2 when compensating controls were considered. A further 70% reported assessing application, equipment and service suppliers.[11] These figures do not measure national continuity. They show that strategies and assessments cannot establish that controls work. ANAO financial-statement audits have also continued to identify deficiencies involving business-continuity planning and testing within broader IT-control findings.[12]

High-consequence systems should be able to enter a safe degraded mode when corporate networks, remote support or ordinary identity services are unavailable. Operators should test isolation points, retain sufficient local authority, restore from trusted source and configuration, recover identity and keys in a defined order, use an alternate update or revocation path and diagnose the system without one unavailable specialist.

Reconstruction may require source code, exact dependencies, build tools, configuration, schemas, firmware, interface specifications, tests, deployment procedures, recovery keys, licensing rights and hardware documentation. Not every system requires public source or escrow. The control should follow consequence, replacement time, supplier viability and legal rights.

Procurement should provide proportionate rights to export data, configuration, logs and identities; operate essential functions during supplier outage; test restoration; obtain security support; transfer maintenance; and replace the service. A contractual exit clause is not effective when proprietary formats, remote control planes or missing knowledge make exit impossible.

Open-source software needs the same discipline. ASD advises manufacturers to identify components, plan for unsupported dependencies and accept responsibility for the software they use.[13] A software bill of materials can identify components but it does not prove support, integrity, recoverability or replacement. Australia should pilot a Critical Software Stewardship Programme for a bounded set of components whose failure would have cross-sector consequences. The pilot should identify consuming functions, maintainers, viable substitutes, provenance, maintenance capacity and an owner prepared to repair or replace the component. Commercial consumers should remain responsible for their use.[14]

Recent failures show that the model must include non-malicious events. The 2024 CrowdStrike update caused widespread outages and required local recovery even after the supplier published remediation. The 2023 Optus outage prevented 2,145 people from accessing Triple Zero and another major emergency-calling outage occurred in 2025. These incidents differ in cause and responsibility but both demonstrate the consequences of concentration, weak observability, failed alternate carriage and difficult recovery.[15][16]

4. Incident coordination, people and communities

Australia has capable incident-response institutions. The unresolved question is whether every national function can reach the right service and whether authority remains clear when several sectors fail together.

The FIRST CSIRT Services Framework is a useful test. A national incident-service map should identify the mandate, constituency, operating hours, alternate contacts, monitoring scope, intake, validation, analysis, coordination, recovery and communication services provided by ASD's Australian Cyber Security Centre (ACSC), CISC, NEMA, sector regulators, jurisdictional teams, major private response capabilities, vendor product-security teams and international peer CSIRTs. It should also show handover between cyber, physical, emergency and law-enforcement incidents.[6]

FIRST deliberately leaves capacity, maturity and quality outside its service framework. Australia should measure them separately. Evidence should include report queues, time to validate and assign an incident, availability of qualified staff, cross-

entity response, restoration outcomes, stakeholder notification, exercise performance and closure of corrective actions. A team which lists a service but cannot provide it during concurrent incidents does not supply national capability.[17]

Information sharing should be authorised before crisis. FIRST's Traffic Light Protocol 2.0 can describe sharing boundaries for sensitive operational information but it does not replace security classification, privacy law or evidence handling. Government, operators, vendors and researchers should know which channels, contacts and release authorities apply when ordinary systems are unavailable.[18]

The incident map should remain federated. One national team cannot possess every sector's knowledge, statutory authority or operational access. The national owner should ensure that no function falls between mandates and that cross-sector decisions have an accountable authority.

People are part of that capability. Each vital function should identify roles which cannot be absent simultaneously, the minimum team for degraded operation, succession, delegation, clearance requirements, sustainable workload and cross-trained replacements. Exercises should remove senior staff, contractors, ordinary premises and remote vendor support. Fatigue and family obligations are operational constraints rather than individual failures.

Australia also needs repair capability: diagnostic equipment, spares, test facilities, technical documentation, fabrication, secure logistics and authorised technicians. Replacement stock without knowledge can remain unusable. Skilled people without parts, licences or authority cannot restore a service. Sovereign capability should mean practical freedom to operate, repair, substitute or reconstruct what matters rather than domestic production of everything.

Commonwealth, state, territory and local arrangements should state who owns each function, when assistance can be requested or directed, how scarce resources are prioritised, which credentials and workers are recognised across borders and how urgent spending is authorised. Private operators should be treated as operational partners without surrendering public authority. Government should state the required outcome and legal basis while operators state their capacity, dependencies and limits.

Community-service organisations support people who might not receive or act on a general warning, need medicine or mobility support, cannot use a digital-only service or rely on trusted local contact. First Nations governments, community-controlled organisations and local leaders should help define warnings, support and recovery for their communities. Exercises should include people with disability, carers and organisations supporting them so that a nominal degraded service is not accepted when it excludes the people who depend on it.

Public guidance should be accessible, multilingual and specific to Australian conditions. It should explain likely service degradation, household and community actions, trusted warning channels and assistance for people unable to prepare independently. Communication during an outage should state affected functions, scope, known facts, uncertainty, required action and the next update time. Reassurance is not an operational update.[19]

5. Exercises, evidence and accountability

Australia should run a recurring National Continuity Exercise against a demanding Defence and civil scenario. It may align with an appropriate Defence activity while retaining separate civil governance and evaluation.

The scenario should combine failures which expose shared dependencies: loss of international connectivity and a domestic carrier, compromise of a cloud or identity provider, unavailable positioning or trusted time, a destructive cyber event during a natural hazard, disrupted fuel and transport, loss of premises and staff, inconsistent public communication and competing civil and military demand for the same capacity.

The exercise should begin from actual capability rather than grant fictional resources. It should use real alternate contacts, representative restoration and decisions under realistic time. Live systems need not be endangered; isolated environments and bounded operational drills can prove whether procedures, artefacts and people work.

Every material finding should have an owner, correction date and retest. Accepted risk should state the authority, reason, duration and consequence. Findings should not disappear when an exercise programme ends or an official changes role.

Parliament should receive an annual National Continuity Report. The public section should identify functions assessed, evidence used, exercises completed, deficiencies by class, overdue corrections and changes in concentration. A protected annex can contain operational detail. This provides accountability without publishing an attack map.

Performance should be measured through outcomes: functions which maintained minimum service, systems restored from controlled inputs, common dependencies corrected, time required to establish a trusted national picture, decisions delayed

by unclear authority, alternate channels which worked and corrective actions which passed retest. Counting plans, meetings, participants or alerts does not prove continuity.

6. International practice and safeguards

Finland's Security Strategy for Society identifies vital functions, assigns strategic tasks to responsible ministries and involves authorities, businesses, organisations and citizens. Finland monitors implementation through an annual Security Report for Society.[20] Sweden places civilian activity within total defence and defines public responsibilities before heightened alert or war.[21]

NATO's seven baseline requirements cover continuity of government, energy, movement of people, food and water, mass casualties, civil communications and transport. The 2026 requirements address physical and digital risk, cascading effects, vendor concentration, supply chains, priority access and regular exercises.[22] Australia is not a NATO member but the requirements remain a useful assessment reference because they connect civilian continuity with support for military operations.

The United Kingdom's Resilience Framework and Action Plan seek assurance across departments, local responders, essential services and privately operated critical infrastructure. The United Kingdom's difficulty in translating strategy into central direction, legislation and public engagement is also a useful warning.[23]

Australia should adapt these models to its federal system, distance, dispersed communities, import dependence, Indo-Pacific position, natural hazards and privately operated infrastructure. International compatibility should support mutual assistance without making an essential Australian decision depend on one foreign institution.

Preparedness can create new risks. A dependency picture can become an attack guide. Emergency authority can outlive its purpose. Priority decisions can exclude people with less influence. Secrecy can conceal incapacity and domestic-capability policy can become indiscriminate protectionism.

Operational information should therefore be collected only where it supports a defined decision or test. Access should be purpose-bound, logged and independently reviewed. Emergency measures should identify their legal basis, trigger, decision-maker, affected rights, record, review and expiry. Public reporting should disclose whether capability exists and who owns an overdue correction without exposing the detail needed to attack it.

Evidence should be obtained once and reused lawfully across related obligations. Small operators, councils and community organisations should not receive the same reporting burden as a national carrier or major infrastructure operator. Where their participation is necessary, government should provide a proportionate method, technical support and funding.

7. Recommendations

I recommend that the Committee:

- ask PM&C to define vital functions, assign owners and publish a strategy connecting existing systems with bounded emergency authority, rights safeguards, independent review and funded community and workforce preparedness;
- recommend that Home Affairs test a National Continuity Capability across three unlike functions before national expansion;
- require controlled continuity records and a protected, federated dependency picture which identifies concentration, substitutability, endurance, priority and restoration conflicts;
- extend CI Fortify's outcome model to high-consequence digital systems, beginning with government systems and procurement and adding regulation only where an impact assessment establishes a residual gap;
- change high-consequence procurement to require proportionate portability, local operating authority, recovery testing, security support, supplier-exit capability, documentation and transferable knowledge;
- pilot a Critical Software Stewardship Programme for a bounded set of components with cross-sector consequences;
- require a national incident-service map using FIRST's service vocabulary plus pre-authorised sharing channels, alternate communications and separate evidence of capacity, maturity and outcomes;
- establish a recurring National Continuity Exercise with assigned corrections, mandatory retest and annual reporting to Parliament through a public account plus a protected operational annex.

Australia does not need another declaration that resilience matters. It needs a continuing account of what must work, what each function depends upon, who can decide when normal arrangements conflict and what evidence establishes that recovery is possible. An essential function should not be called resilient until it has operated or been representatively restored under the conditions expected to break it.

References

[1] Department of Defence, *2026 National Defence Strategy and 2026 Integrated Investment Program*, 2026.

[2] Department of the Prime Minister and Cabinet, *Australian Government Crisis Management Framework*, September 2025.

[3] Department of Home Affairs, *Australian Disaster Preparedness Framework*, accessed 4 November 2026.

[4] Cyber and Infrastructure Security Centre, *SOCI Act regulatory obligations*; *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, compilation effective 10 June 2026, especially ss 4A, 6A and 8A to 11A.

[5] Australian Signals Directorate, *CI Fortify: Guidance for Australian critical infrastructure service continuity and resilience*, 13 October 2025.

[6] Forum of Incident Response and Security Teams, *CSIRT Services Framework, version 2.1*, accessed 4 November 2026.

[7] Parliamentary Joint Committee on Defence, *Inquiry into Australia's national civil preparedness and resilience* and terms of reference, 2026.

[8] Department of the Prime Minister and Cabinet, *Australian Government Crisis Management Framework: Purpose*, accessed 4 November 2026.

[9] Productivity Commission, *Vulnerable Supply Chains*, Study Report, July 2021; Department of Industry, Science and Resources, *Office of Supply Chain Resilience*, accessed 4 November 2026.

[10] Infrastructure Australia, *A Pathway to Infrastructure Resilience*, 2021, especially pp. 39 to 40.

[11] Australian Signals Directorate, *The Commonwealth Cyber Security Posture in 2025*, February 2026, especially pp. 11 and 18.

[12] Australian National Audit Office, *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2025*, especially paras 3.45 to 3.50.

[13] Australian Signals Directorate, *Choosing secure and verifiable technologies*, May 2024; Australian Signals Directorate and international partners, *A Shared Vision of Software Bill of Materials for Cybersecurity*, September 2025.

[14] United States Cybersecurity and Infrastructure Security Agency, *Open Source Software Security Roadmap*, September 2023.

[15] Australian Signals Directorate, *Widespread outages relating to CrowdStrike software update*, 19 to 21 July 2024.

[16] Australian Communications and Media Authority, *Optus pays $12 million penalty for Triple Zero outage*, 8 November 2024; *ACMA takes Optus Mobile to court over September 2025 Triple Zero outage*, July 2026.

[17] Forum of Incident Response and Security Teams Metrics SIG, *Metrics for the CSIRT Services Framework, version 1.1*, 2026.

[18] Forum of Incident Response and Security Teams, *Traffic Light Protocol, version 2.0*, authoritative from August 2022.

[19] Australian Signals Directorate and international partners, *Communicating under pressure: Best practices for service providers*, October 2026.

[20] Security Committee of Finland, *Security Strategy for Society*, adopted 16 January 2025.

[21] Swedish Civil Contingencies Agency, *Strengthening civil preparedness*, accessed 4 November 2026.

[22] North Atlantic Treaty Organization, *2026 Resilience Baseline Requirements*, 15 September 2026.

[23] United Kingdom Cabinet Office, *UK Government Resilience Action Plan*, July 2025; *The UK Government Resilience Framework*, December 2022; House of Lords Library, *UK civil preparedness for war: Government strategy*, 19 March 2026.