Transformory Submission to the Triple Zero Custodian's Triple Zero Legislative and Regulatory Review

Triple Zero Custodian
Australian Government Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

June 2026

Status: This submission may be made public

TRANSFORMORY PTY LTD (ABN 24 610 810 716)
[redacted]
www.transformory.com

Contact: David Burns, Managing Partner
[redacted]

Transformory acknowledges the Traditional Custodians of Country throughout Australia and recognises their continuing connection to land, waters and culture, including in cyberspace. We pay our respects to Elders past, present and emerging.

Table of Contents

Statement of interest

In March 2026 Transformory wrote to the Minister offering to undertake a paid national architecture scoping study. In April 2026 the Department declined that unsolicited offer and directed the firm to this public consultation. While Transformory has a commercial interest in advisory work in emergency communications and telecommunications regulation, this submission is offered as public-interest input to the Review and is not a re-proposal of that engagement. This submission may be made public.

Executive summary

Transformory welcomes the Review and supports its objective of a Triple Zero framework that is fit for purpose, now and into the future. This submission responds to the questions raised in the Consultation Paper, in the order the paper poses them, and frames its answers as a set of strategic decisions the Commonwealth can take to move Triple Zero from a collection of well-run components toward a measured, resilient national capability.

Our central proposition is narrow and within scope. The major recent failures were not, in the main, failures of missing rules. They were failures of two kinds: reliability is not an express, measured objective of the networks Triple Zero depends on, and the framework regulates components rather than the end-to-end call chain. The reforms since the Bean Review (the Custodian, outage-communication rules, mandatory testing, camp-on and fall-back obligations, welfare checks, and a $30 million maximum penalty) close real gaps, but they remain largely component-level and outcome-stated rather than system-level and performance-measured.

A second observation runs through the record. Australia has not lacked expert advice on Triple Zero; successive Commonwealth and State reviews have produced sound recommendations (Attachment D). What the system has lacked is a standing assurance that those recommendations are carried through to verified, durable implementation. The disciplined acquittal of the Bean Review — 17 of its 18 recommendations implemented or significantly progressed — shows what good looks like; the discipline should be made permanent rather than an artefact of any single review.

International experience confirms both the destination and the delivery risk. The United Kingdom's Emergency Services Network and the United States' FirstNet show that federal leadership, legislative clarity, defined spectrum and measured performance can deliver priority and resilience for public-safety communications; they also show, in the UK case, how cost and schedule discipline can be lost without it (Attachment B). The Australian record shows the same lesson from the other direction: where reliability is assumed rather than measured, the system fails under stress, and the consequences extend well beyond the headline outage into coronial inquests and civil litigation (Attachment C).

We distinguish throughout between what is established (proof), what we infer, and what is aspiration. The broader question of a nationally integrated public-safety communications architecture is, in our view, the strategic horizon these reforms serve; we treat it only briefly under Other matters, and we do not ask the Review to widen its scope to reach it.

A note on the current Senate Committee inquiry, and how this submission relates to it

This submission is informed by, and is intended to complement, the substantial body of evidence assembled by the Commonwealth Senate Environment and Communications References Committee in its inquiry into Triple Zero service outages. That inquiry has undertaken detailed and valuable work including public hearings and written submissions from the carriers, the parent company of Optus (Singtel), device manufacturers, network vendors, the regulator, the Department including the Triple Zero Custodian, consumer and industry bodies, and Commonwealth and State emergency-management and response agencies. We acknowledge that work and have drawn on the public record where it sharpens the evidence base for this Review.

Noting the Committee's final report is due to be tabled on 30 June 2026, after submissions to this Review close, our submission anticipates rather than restates the Committee's findings, and we encourage the Review to read the two processes together: the Committee's forensic account of what happened on and around 18 September 2025, alongside the structural, framework-level decisions this submission identifies to ensure such failures are prevented, measured and assured against in future.

Summary of our recommendations for a resilient Triple Zero service

The table below consolidates our recommendations developed in the body of this submission, posed as what we believe them to be: strategic decisions. For each, we note whether it requires financial investment, regulatory change, and/or a change to existing delegations or the creation of new authority. The detail, and the consultation question and instrument each maps to, is set out in the submission's sections that follow.

#	Strategic decision	Investment (source)	Regulatory change (level)	Changed/ new authority
1	Make reliability and resilience express, measured objectives of the framework (not implied consequences of access).	—	Federal	—
2	Adopt enduring, technology-neutral principles and a standing mechanism to admit new access methods against published criteria.	—	Federal	New (federal)
3	Convert prioritisation and redundancy (camp-on / inter-network fall-back) from assumed outcomes into measured obligations that hold under surge.	Industry (possible co-investment)	Federal	—
4	Define end-to-end network performance standards and attach them to carriers and CSPs, not only the Emergency Call Person. (The single most consequential decision.)	Industry + Federal	Federal	New (federal)
5	Bring devices and manufacturers into the framework; establish a device-capability register and a class-level gatekeeping power.	Industry + Federal	Federal	New (federal)
6	Build layered proactive assurance: independent measurement, pre-change testing, independently verified post-incident plans, and audit powers.	Federal + industry	Federal	New (federal)
7	Establish standing, standardised end-to-end performance reporting across all call-chain providers, with an annual public report.	Industry + Federal	Federal	New (federal)
8	Establish standing information-sharing governance and timely outage-scope and location data to emergency service organisations.	Federal + industry (possible co-investment)	Federal	New (federal)
9	Specify a robust, measured Commonwealth baseline plus interoperability and interface standards so State innovations attach consistently.	Federal + State (possible co-investment)	Federal	—

#	Strategic decision	Investment (source)	Regulatory change (level)	Changed/ new authority
10	Give ACMA an explicit proactive mandate to set and enforce performance standards and to aggregate related incidents into systemic findings.	Federal	Federal	New (federal)
11	Clarify the ACMA–Custodian interface, add a standing standards-setting pathway, and confirm the Custodian's authority, resourcing and independence.	Federal	Federal	Change (federal)
12	Make implementation assurance an enduring Custodian function — a published, periodically verified register of review and inquiry recommendations and their status.	Federal	Federal	New (federal)

Key. Financial investment names the likely source(s): private industry (carriers and device manufacturers), the federal government (regulator and Custodian capacity, registers, independent measurement) and/or state government; "—" means none beyond drafting. Regulatory change and authority are at the federal (Commonwealth) level in every case: the Triple Zero framework is Commonwealth law, and these decisions are deliberately designed to require no change to State legislation (Decision 9 affects how State innovations attach, but changes no State law). "New" = a new authority or function; "Change" = a change to existing delegations; "—" = none required.

A note on the basis of this classification. The table reflects where each lever currently sits in the framework. That is the right baseline – but it assumes the present allocation is itself the right one. Several of these decisions are also an opportunity to challenge or evolve the status quo: who should fund resilience that benefits the whole community; whether an authority that is federal today should be exercised jointly with the States; and whether new shared (co-investment) arrangements would better match responsibility to benefit. Where we see that funding opportunity most clearly, the table marks "(possible co-investment)". Re-allocating a lever is itself a strategic decision, and connects to the strategic horizon noted below.

Strategic horizon – recorded, not recommended for this Review

Priority access, pre-emption and network segmentation for public-safety communications – as delivered by the UK's ESN and US FirstNet and contemplated by Australia's Public Safety Mobile Broadband agenda – would require major financial investment, regulatory and spectrum change, and new authority. It is broader than this Review. We record it as the strategic horizon the in-scope decisions above and the likely outcomes of the Senate Inquiry would serve; we do not ask the Custodian to determine it.

1. Methods of access for Triple Zero (Consultation Paper section 2)

1.1 Principles to guide regulation in the contemporary environment (Q1)

The framework's founding principle – reasonable and equitable access, free of charge – remains sound, but it was built for a fixed-line world in which most call functionality sat in the network. With more than 85 per cent of calls now made from mobile devices, and with call functionality distributed across devices, carriers and the Emergency Call Person, access alone is no longer a sufficient organising idea.

The framework should be anchored in a short set of enduring, technology-neutral principles:

- reliability and resilience as express objectives, not implied consequences of access;
- end-to-end accountability across the whole call chain;
- technology-neutrality and adaptability, so new access methods are accommodated by principle rather than by repeated bespoke amendment;
- the appearance and the substance of a single national system for the end user; and
- equity of access, including for users of the National Relay Service and in regional and remote areas. These belong in the objects of the TCPSS Act and should cascade into the ECS Determination.

Strategic decision 1. Add reliability and resilience as express objectives of the Triple Zero framework, alongside access, in the TCPSS Act and the ECS Determination. This is a regulatory-drafting decision; it requires no new investment or authority, but it is the keystone on which the measured obligations below depend.

Strategic decision 2 (principles). Adopt a short set of enduring, technology-neutral principles – including end-to-end accountability and the single-national-system objective – as the stated basis of the framework, supported by a standing delegated mechanism to admit new access methods. This requires regulatory change and a modest new delegated authority (below).

1.2 Barriers to new access technologies (Q2)

The framework is expressed around voice telephony over fixed-line or mobile services. Emerging access methods – vehicle eCall, fall-detection wearables, satellite messaging, and Low Earth Orbit direct-to-device services supported by the proposed Universal Outdoor Mobile Obligation – do not map cleanly onto that definition, which both leaves users uncertain of their protection and risks ad hoc treatment. The barrier is definitional and procedural rather than substantive.

Strategic decision 2 (access). Make the access definition technology-neutral and create a standing mechanism – a determination power – to admit new access methods against published reliability, integrity and locatability criteria, without primary-law amendment for each new technology. This is regulatory change plus a new standing delegation to ACMA (on the Custodian's advice).

1.3 Balancing multi-modal access against reliability and redundancy (Q3)

Multi-modal access widens reach but multiplies failure modes and the risk of non-genuine calls. The September 2025 Optus outage is the instructive Australian case: redundancy existed in principle (camp-on to another network) but performed poorly in practice.

> Case study: September 2025 Optus outage (systemic reliability failure)
>
> What happened: a firewall upgrade applied under the wrong change plan caused roughly 75% of more than 600 Triple Zero calls to fail across the NT, SA, far-west NSW and WA over about 13-15 hours. The independent Schott Review found camp-on to an alternate network could take 40-60 seconds and frequently did not succeed.
>
> Why it matters: redundancy was assumed to work but was never measured. Up to four deaths were initially linked to the outage, with two later linked by police. This is the clearest evidence that redundancy must be specified as a measured obligation, not an assumed outcome.
>
> Full case study: Attachment C, C.4.

The lesson is not to slow innovation but to measure redundancy. A new access mode should be admitted only against the reliability and integrity criteria above; and redundancy mechanisms such as camp-on and fall-back should be treated as measured performance obligations – with stated success-rate and latency thresholds – rather than as outcomes assumed to work. Reliability must also be specified for the conditions in which Triple Zero is most needed: natural disasters, major incidents and mass-casualty events concentrate extreme, simultaneous demand at the very moment access matters most.

Strategic decision 3. Treat prioritisation and redundancy (camp-on and inter-network fall-back) as measured performance obligations with explicit success-rate and latency thresholds in the ECS Determination, defined to hold under surge and congestion. This requires regulatory change and carrier investment in network capability and testing.

1.4 Device-class gatekeeping by ACMA or the Minister (Q4)

We support a clear, transparent power for ACMA, on the Custodian's advice, to determine classes of devices or technologies that may or may not access Triple Zero, exercised on published criteria and subject to review.

> Case study: the post-3G handset problem (systemic, slow-burn failure)
>
> What happened: after the 3G shutdown, certain software-incompatible 4G handsets cannot complete or camp-on for Triple Zero, and such failed attempts can be invisible to carriers. One carrier (TPG Telecom) initially advised the regulator that blocking individual device identifiers was not operationally feasible, then implemented blocking as device-related failures emerged. A prominent November 2025 case initially reported as a death linked to an outdated handset was subsequently disputed (see Attachment C).
>
> Why it matters: the device and manufacturer layer is now load-bearing for Triple Zero outcomes but sits largely outside the framework, and there is no orderly mechanism to manage eligibility at the class level.
>
> Full case study: Attachment C, reference 6.

Strategic decision 5 (gatekeeping). Provide a transparent, criteria-based power for ACMA (advised by the Custodian) to determine classes of devices or technologies permitted or excluded from Triple Zero access — a preventive complement to the existing Part 4 power to block individual devices. Regulatory change plus a new class-level authority.

1.5 Device manufacturers and a device register (Q5)

Yes, device manufacturers should be considered more centrally. The move to all-IP networks shifted material emergency-calling functionality into device software and firmware, so manufacturers are now load-bearing for Triple Zero outcomes while sitting largely outside the ECS Determination and being addressed mainly through the Labelling Notice and the regulatory compliance mark.

Strategic decision 5 (manufacturers and register). Bring device manufacturers within the framework and establish a mandatory device-capability and emergency-calling register, maintained by or for ACMA, to support Part 4 blocking, give carriers and consumers a reliable reference, and provide the evidentiary base for admitting new access methods. Regulatory change, a new register (modest investment), and a new standing authority to maintain it.

2. Industry obligations (CP section 3)

2.1 Outcomes and minimum requirements for carriers, CSPs and ECPs (Q6)

The outcomes the Determination already states – for example, that an emergency call must be carried to the relevant termination point (s 19) – are the right outcomes. The deficiency is that, for carriers and CSPs, these outcomes are stated but not measured: there are currently no performance standards for the networks that carry Triple Zero calls.

> Case study: 1 March 2024 Telstra CLI fault (isolated operational-discipline failure)
>
> What happened: a Calling Line Identification (CLI) platform fault on 1 March 2024, triggered by a surge of medical-alert IoT-device registrations, meant that of 494 inbound Triple Zero calls over about 90 minutes, 148 were not successfully transferred; Telstra's stored backup numbers for emergency services were also incorrect. A Victorian man in cardiac arrest died after his call was not transferred and ambulance dispatch was delayed. ACMA found 473 breaches and penalised Telstra more than $3 million.
>
> Why it matters: this was an operational-discipline failure within a single provider rather than a gap in the rules – but it shows why end-to-end outcomes (CLI and location integrity, transfer success) must be measured, not assumed.
>
> Full case study: Attachment C, reference 7.

We recommend defining a small set of end-to-end outcomes – call connection or completion, camp-on success and latency, CLI and location integrity, and restoration time after disruption – and attaching minimum performance standards and measurement to each, specified to hold under peak and emergency-driven demand. This is the in-scope form of the Review's own Matter for Consideration on minimum mobile network performance standards.

Strategic decision 4. Define a small set of end-to-end outcomes and attach minimum network performance standards and measurement to carriers and CSPs, not only the Emergency Call Person. This is the single most consequential change available to the Review. It requires regulatory change (a new performance standard), carrier investment in capability and measurement, and a clear authority for ACMA to set and assure the standards.

2.2 Proactive identification and rectification of systemic issues (Q7)

The September 2025 outage shows that detection failed before rules failed: the carrier's volume monitoring excluded Triple Zero calls so no alarm was raised, several contact-centre notifications were not escalated, and emergency services and regulators were told only after the fault was resolved. Mechanisms that depend on a provider noticing and reporting its own failure are the weakest; mechanisms built on independent measurement and verification are the strongest.

We recommend a layered approach, in order of effectiveness: (1) minimum performance standards with independent measurement, so systemic underperformance is visible without relying on self-report; (2) mandatory pre-change testing and management plans for changes that could affect Triple Zero (building on Division 5.3 of the Determination, whose adequacy the Review should test); (3) mandatory post-incident improvement plans (now legislated) with independent verification rather than self-attestation; and (4) ACMA powers to compel targeted audits and to aggregate related incidents into systemic findings.

Strategic decision 6. Mandate layered proactive mechanisms – independent measurement, pre-change testing and management plans, independently verified post-incident improvement plans, and audit

powers – prioritising measurement over self-report. Regulatory change, some investment in independent verification and audit capacity, and new compel/audit authority for ACMA.

2.3 Performance reporting and metrics (Q8)

Reporting today centres on the Emergency Call Person, which captures only one segment of a chain that may cross several providers. The ECS Directions the Custodian requested on 17 April 2026, requiring the three Mobile Network Operators to provide Triple Zero call-delivery data, are an excellent template – but they should be converted from ad hoc directions into a standing obligation. Suggested metrics: call-attempt and connection-success rates by network and region; camp-on success rate and latency; CLI and location accuracy; time from outage onset to detection and to notification; and welfare-check completion.

Strategic decision 7. Establish standing, standardised Triple Zero network-performance reporting across all call-chain providers, building on the 17 April 2026 ECS Directions, with defined metrics, regular aggregate reporting, immediate incident reporting, and an annual public report. Regulatory change, modest investment, and a standing reporting authority.

2.4 Information sharing and governance (Q9)

The real-time outage-information amendments in force from 1 November 2025 are a sound base. What is missing is standing governance so that sharing is routine and structured rather than triggered case by case: agreed data definitions, secure channels, and clear roles among the Mobile Network Operators, the Emergency Call Person, ACMA, the Custodian and emergency service organisations. The Custodian is the natural steward. This is also where the integration deficiency can be addressed within scope – through shared information rather than shared infrastructure.

Strategic decision 8 (governance). Establish standing information-sharing governance across the Triple Zero ecosystem – data definitions, secure channels and roles – stewarded by the Custodian. Regulatory change, modest investment in secure channels, and a clarified stewardship authority.

3. The framework's impact on emergency service organisations (CP section 4)

3.1 The single national system and State and Territory innovation (Q10)

The objective of a single national system, as experienced by the end user, is correct and should be retained. Properly specified, a high and measured Commonwealth baseline enables rather than hinders State innovation: New South Wales' BluLink video and location-sharing capability, for example, is built on top of the baseline call. The risk runs the other way – if the Commonwealth baseline is under-specified, jurisdictions fill the gaps inconsistently, which entrenches the fragmentation the Review is concerned about.

> Case study: Victoria's 000 call-answer crisis (systemic capacity failure at the State layer)
>
> What happened: between late 2021 and early 2022 the Victorian call-taker (ESTA) could not answer emergency calls within target. In October 2021 only 47.4% of ambulance calls were answered within five seconds (target 90%); by January 2022 the figure was 39%, with some callers waiting more than ten minutes.
>
> Why it matters: the Commonwealth front-end functioned, but the State call-answer layer failed under demand because of its funding model. The IGEM review (Sept 2022) made 42 findings and 8 recommendations; the Ashton Capability and Service Review (May 2022) made 20, prompting a $333m funding package and the rebrand to Triple Zero Victoria. It is the clearest example that a national service is only as resilient as its weakest jurisdictional layer.
>
> Full case study: Attachment C, reference 8; review detail: Attachment D.

Strategic decision 9. Specify a robust, measured Commonwealth baseline and publish interoperability and interface standards so State and Territory innovations attach to the national service consistently. Consistent with the Terms of Reference, this is a Commonwealth-baseline and interface decision; we make no recommendation to change State or Territory legislation. Regulatory change and standards work; some investment; no change to State authority.

3.2 Carrier-held information that should reach ESOs (Q11)

Carriers and the Emergency Call Person hold information that emergency service organisations need in real time for resourcing and welfare response: the scope and affected area of an outage, the networks and locations involved, and best-available caller location and CLI.

Strategic decision 8 (data to ESOs). Regulate the timely provision of outage-scope and best-available location data to emergency service organisations during incidents, extending the 1 November 2025 base and operating under the information-sharing governance above. Regulatory change and modest investment.

4. Proactive regulatory oversight (CP section 5)

4.1 Additional ACMA powers for proactive, future-focused regulation (Q12)

ACMA's information-gathering and general powers are broad, but they are oriented to investigation and enforcement after a failure rather than to setting and assuring reliability in advance. ACMA needs an explicit mandate to set and enforce minimum performance standards for Triple Zero carriage and to require standing performance reporting – a proactive reliability-regulation function, not only a post-incident investigatory one.

Strategic decision 10 (proactive mandate). Give ACMA an explicit proactive mandate to set and enforce minimum performance standards for Triple Zero carriage and to require standing performance reporting. Regulatory change and a new proactive authority; some regulator-capacity investment.

4.2 Systemic issues and linking related infringements (Q13)

The recurrence of the same failure modes across providers – camp-on latency and device-compatibility problems affecting more than one carrier – indicates these are systemic rather than discrete matters.

Strategic decision 10 (systemic findings). Empower and require ACMA to aggregate related incidents into systemic findings and to act on patterns across providers, informed by the Custodian's whole-of-ecosystem view, rather than being confined to treating each breach in isolation. Regulatory change and a new aggregation authority.

4.3 Balance between ACMA as regulator and the Custodian as overseer (Q14)

The regulator/overseer split introduced by the 2025 Act is sound and worth preserving: the Custodian provides direction, standards advice and ecosystem oversight; ACMA holds enforcement. The mechanism by which the Custodian requests an ECS Direction (s 151L) is useful but is incident-driven by design. It should be complemented by a standing standards-setting pathway, so that reliability is set and assured continuously, and the interface between the two bodies should be clarified to avoid both duplication and gaps.

Strategic decision 11 (interface). Clarify the ACMA–Custodian interface and add a standing standards-setting pathway alongside the incident-driven section 151L mechanism. Regulatory change and clarified delegations.

4.4 Whether the Custodian has the powers it needs (Q15)

On the face of the 2025 Act, the Custodian's powers appear broadly adequate. We infer, rather than assert, that three things would strengthen the role: explicit standing authority to require system-wide performance data; a clear mandate over end-to-end (whole-call-chain) performance, not only oversight of components; and resourcing and independence sufficient to sustain a genuinely proactive function.

Strategic decision 11 (Custodian authority). Confirm the Custodian's standing authority over end-to-end performance data and ensure resourcing and independence sufficient for a proactive role. Regulatory clarification, confirmed/expanded delegations, and investment in the Custodian's capacity.

4.5 Ensuring reform is cumulative: implementation assurance (Additional Matter for Consideration)

The Terms of Reference rightly include, as a Matter for Consideration, the effectiveness of implemented Optus Outage Review recommendations. We suggest this be read broadly. The Triple Zero system has been examined repeatedly and well –across the Commonwealth and the States (Attachment D) – but has historically lacked a standing assurance that recommendations are implemented and stay implemented. Disaster roaming, recommended since 2020, is still not operational; Optus failed welfare checks again in 2025 although the rules existed. Where assurance is present (as in the structured acquittal of the Bean Review) reform compounds; where it is absent, the benefit of expert review can be lost between reviews, and the same issues are revisited after the next incident.

Strategic decision 12. Make implementation assurance an explicit, enduring part of the Custodian's mandate – a transparent, periodically verified and published register of recommendations from relevant Commonwealth and State reviews, inquiries and major-incident investigations and their implementation status – so that reform is cumulative rather than episodic. Regulatory change, a new standing function, and modest investment in the Custodian's capacity.

5. Other matters (CP section 6)

Taken together, the in-scope decisions above – reliability as an express objective, end-to-end measurement and reporting, standing information-sharing governance, and systemic oversight – move the system from a set of well-run components toward a measured, integrated national capability. That direction is, in our assessment, an inference and an aspiration rather than an established finding, and we frame it as such.

International practice answers the underlying problem by giving public-safety users priority access and pre-emption on the network – in effect a protected transit lane that continues to function when networks are congested. The two leading models, summarised below and detailed in Attachment B, show both what success looks like and how delivery discipline matters.

Case study summary: United Kingdom Emergency Services Network (ESN)

Model: a nationally mandated 4G public-safety network replacing legacy Airwave radio, run over EE/BT commercial infrastructure under Home Office mandate, with IBM as lead system integrator.

Measures of success: coverage of c. 20,840 sites including ~1,045 new masts and 292 purpose-built masts for the most remote areas (Extended Area Service); voice, video and data for first responders.

Cautionary measure: cost has roughly doubled to an estimated ~£11.3bn (2024) and completion has slipped to 2029 – a decade late – with the National Audit Office and Public Accounts Committee citing significant avoidable costs. Federal leadership without delivery discipline is expensive.

Full case study: Attachment B, case study 1.

Case study summary: United States FirstNet

Model: a dedicated public-safety broadband network created by Congress in 2012, with allocated spectrum (Band 14) and a public-private partnership with AT&T, providing priority and pre-emption to first responders.

Measures of success: 7 million+ connections across nearly 30,000 public-safety agencies; coverage approaching 3 million square miles (+20,000 sq mi in 2024 alone); 1,000 new sites in 2024–25 and 11,000+ in-building sites; nationwide buildout completed 2023; ~$2bn reinvested in network evolution.

Federal roles: governed by the FirstNet Authority (Department of Commerce), delivered by AT&T, and relied on operationally by FEMA – whose emergency-communications role differs markedly from Australia's NEMA.

Lesson: dedicated spectrum, statutory clarity and measured, published outcomes can deliver resilient priority communications at national scale.

Full case study and the FEMA/NEMA comparison: Attachment B, case study 2.

Taken with the recurring outages documented in Attachment C, this is, in our assessment, evidence of a structural case for priority access, pre-emption and network segmentation for emergency communications. We frame this as an inference from the evidence rather than a finding. Together with the wider questions of national public-safety communications architecture and spectrum strategy it is broader than the present Review, and we do not ask the Review to determine it; we record it as the strategic horizon that the in-scope decisions in this submission would serve.

The terrorist attack at Bondi Beach on 14 December 2025 was, above all, a tragedy, and is now the subject of a Royal Commission, which is the proper forum for any findings about the response; we draw no conclusion about that day. The wider point is structural: mass-casualty incidents place concentrated, simultaneous demand on the same commercial networks that carry Triple Zero and on which response agencies increasingly depend – and those networks have repeatedly proven fragile under far less stress.

ATTACHMENT A: About the submitter

Transformory Pty Ltd is an independent advisory firm working with government and industry on strategy, policy and operating models for mission-critical environments. This submission is made by the following contributors

David Burns (Managing Partner) has over 35 years in technology and telecommunications across Australia, the United Kingdom, the United States and Asia. In recent roles he led the delivery of emergency services network systems across Australian jurisdictions, including the integrated network deployed in Tasmania, and has worked extensively with carriers, emergency service agencies and government on the design and operation of mission-critical communications. His career spans senior executive leadership in enterprise and global business services, large-scale network delivery, and the practical realities of large-scale incident response.

Ben Meek (Co-founder) is a data scientist and a strategy and digital leader with deep experience in critical national infrastructure. His experience includes the original establishment of operational and business support systems at Optus in the early 1990s and current post-event recovery work with a large United States public utility. He served pro bono for six years as a founding member of the Parramatta Smart City committee and brings a data- and evidence-led approach to questions of network reliability, resilience and measurement.

Dr Rob Nicholls brings four decades in telecommunications regulation, competition law and technology policy. He was a General Manager at the Australian Competition and Consumer Commission (ACCC) with responsibilities including telecommunications transmission, facilities access, spectrum and mobile services. He served as Australia's Independent Telecommunications Adjudicator from 2012 to 2020 and is a Senior Research Associate at the University of Sydney. His work focuses on the intersection of competition, regulation and technology in telecommunications markets, including the regulatory design questions at the centre of this Review.

ATTACHMENT B: International case studies

This attachment sets out, as case studies, the two international public-safety communications models referenced above, with their governance, funding and measures of success. Both show the value of federal leadership, legislative clarity and measured performance; the UK case also shows the cost of weak delivery discipline. Figures are drawn from official and contemporaneous public sources (see Attachment E).

1. United Kingdom – Emergency Services Network (ESN)

ESN is a nationally mandated mobile-broadband network intended to replace the legacy Airwave TETRA radio system used by UK police, fire and ambulance services. It is delivered under the Home Office's Emergency Services Mobile Communications Programme (ESMCP). The Home Office sets the mandate and standards; the network runs over commercial 4G infrastructure (EE/BT) but is architecturally distinct from consumer traffic, with dedicated core capability to prioritise and manage public-safety traffic.

Governance and delivery model

In December 2024, EE was confirmed to provide the mobile communications infrastructure; in January 2025 IBM was announced as lead for design, build and system integration (a contract of c. £1.63 billion). In August 2024, the Home Office signed a c. £2.22 billion connectivity agreement with BT/EE. Delivery is therefore a government-mandated, systems-integrator-led model under long-term contract.

Measures of success

- Coverage: a total of c. 20,840 new and upgraded sites planned across Great Britain, including 19,795 upgraded EE sites and c. 1,045 new 4G masts, plus 292 purpose-built masts for the most rural and remote areas (the Extended Area Service).
- Capability: fast, secure voice, video and data over 4G, giving first responders immediate access to data, images and information during incidents – capability legacy radio cannot provide.
- Architecture: priority and dedicated core capability that segments public-safety traffic from consumer traffic during major incidents.

Cautionary measures: delivery discipline

ESN is a lesson in delivery risk as much as ambition. The most recent overall delivery-cost estimate (March 2024) is c. £11.3 billion – roughly double original projections – and the scheduled completion date has slipped to 2029, about a decade later than first planned. The National Audit Office and the Public Accounts Committee have repeatedly criticised cost and schedule, noting significant avoidable costs to emergency services (for example forces spending an estimated £125 million since 2018 maintaining Airwave, with c. £25 million more expected by 2026). For Australia the lesson is twofold: federal mandate and dedicated capability are achievable, but only disciplined governance, realistic scheduling and measured milestones keep them affordable.

2. United States

2.1 FirstNet and FEMA

FirstNet arose directly from the communications failures between agencies exposed by the 9/11 Commission. In 2012 Congress created the First Responder Network Authority (FirstNet Authority) and allocated dedicated public-safety spectrum (Band 14) and funding to build a nationwide public-safety broadband network. It operates as a public-private partnership with AT&T, providing priority and pre-emption so first responders retain access even during network congestion.

Governance and delivery model

The FirstNet Authority – an independent authority within the National Telecommunications and Information Administration (NTIA) in the Department of Commerce – holds the spectrum licence and sets requirements; AT&T builds and operates the network under a long-term agreement, funded by an initial federal investment and ongoing reinvestment. The Authority directs continued buildout and, in recent decisions, has approved c. US$2 billion for network evolution and new purpose-built sites. Notably, the network's governance sits with the FirstNet Authority and AT&T rather than with the Federal Emergency Management Agency (FEMA), whose distinct operational role is set out below.

Measures of success

- Adoption: 7 million+ connections (early 2025, up from c. 5.5 million in 2024) across nearly 30,000 public-safety agencies and organisations.
- Coverage: approaching 3 million square miles, having added c. 20,000 square miles in 2024 alone; the initial nationwide buildout was completed in 2023, with 1,000 new sites launched across 2024–25.
- Resilience and indoor coverage: more than 11,000 miniature/in-building cell sites deployed to strengthen coverage in public-safety facilities, plus deployable assets and satellite connectivity.
- Core capability: priority and pre-emption on Band 14, so public-safety traffic is protected when commercial networks are congested.

Lesson for Australia

FirstNet shows that dedicated spectrum, statutory clarity and a measured, publicly reported set of outcomes (connections, agencies, coverage, in-building sites) can deliver resilient priority communications at national scale within roughly a decade of legislation. The published metrics also model the kind of standing, transparent performance reporting this submission recommends for Triple Zero.

2.2 The role of FEMA, and how it differs from Australia's NEMA

A feature of the US model that has no clean Australian equivalent is the role of the Federal Emergency Management Agency (FEMA), part of the Department of Homeland Security. FEMA does not own or operate FirstNet – that governance sits with the FirstNet Authority and AT&T – but FEMA is one of the network's most significant federal users and, more importantly, is the operational federal owner of emergency communications in the United States.

Under Emergency Support Function #2 (Communications) of the National Response Framework, FEMA coordinates the restoration and deployment of communications after a catastrophic loss of local and regional services, including through deployable assets such as Mobile Emergency Response Support (MERS). FEMA also operates the Integrated Public Alert and Warning System (IPAWS) – the national channel for Wireless Emergency Alerts, the Emergency Alert System and NOAA weather radio – used by more than 1,600 federal, state, local, tribal and territorial alerting authorities.

The effect is that, although responsibility in the US is spread across agencies – the FirstNet Authority (within the Department of Commerce's NTIA) for the dedicated network and spectrum, AT&T for delivery, and FEMA for operational coordination and public alerting – each layer has a clear federal owner, and the operational emergency-management agency (FEMA) is wired directly into the public-safety communications system as both a major user and the federal communications coordinator of last resort.

Australia's National Emergency Management Agency (NEMA) occupies a markedly different position. While NEMA leads and coordinates national action across the emergency-management continuum for nationally significant, cross-jurisdictional crises, and administers Commonwealth disaster recovery assistance, NEMA has no role in the Triple Zero regulatory framework, and no operational ownership of the telecommunications-resilience levers that determine whether emergency calls connect. These sit in the Communications portfolio with the Department, ACMA and the Triple Zero Custodian. Unlike FEMA, NEMA neither operates a national public-safety communications network (Australia has no FirstNet equivalent) nor holds regulatory or assurance powers over the networks that carry Triple Zero, nor runs the national public-alerting system (in Australia, emergency alerting is delivered through separate Commonwealth and State arrangements rather than a single NEMA-run platform).

NEMA's own evidence to the Senate inquiry confirms this division precisely. In her 26 February 2026 statement, the Deputy Coordinator-General set out that, under the Australian Government Crisis Management Framework, the Department (DITRDCSA) is the Lead Coordinating Agency for telecommunications outages and the Triple Zero Custodian sits within it, while NEMA is an 'enabling agency' whose National Situation Room provides 24/7 situational awareness and can convene a National Coordination Mechanism at the lead agency's request.

NEMA, she stated, 'does not bear responsibility for operating networks, regulating telcos, managing devices, or notifying the public', and does not hold the direct industry-engagement mechanisms the Department holds. This is the clearest possible confirmation that coordination and regulatory assurance sit in different hands – and why the explicit interface and standing information-sharing arrangements in Strategic decisions 8 and 11 are needed to join them.

This institutional difference matters for the Review. In the United States, the operational emergency-management agency is structurally connected to public-safety communications – as user, coordinator and alerting authority – even though network governance sits elsewhere. In Australia the national emergency-management coordinator (NEMA) and the bodies that regulate and assure Triple Zero reliability (ACMA and the Custodian) are institutionally separate, and no single body owns end-to-end public-safety communications.

That separation is not, in our view, an argument for merging functions. It is an argument for the explicit interface and standing information-sharing arrangements recommended in this submission (Strategic decisions 8 and 11), so that NEMA's whole-of-continuum coordination role and the Custodian's end-to-end reliability mandate are deliberately joined – particularly during the disasters and mass-casualty events when emergency communications are under the greatest stress – rather than left to operate in parallel.

3. Other models and the domestic precedent

Other federations are on similar paths, for example South Korea's nationwide dedicated public-safety LTE network (Safe-Net) and Canada's public-safety broadband planning – and Australia has a domestic precedent in Tasmania's integrated emergency-services network. We do not set out verified comparative metrics for these here and flag them as areas for further evidence rather than relying on unverified figures, consistent with the evidentiary discipline of this submission. The common characteristics across all credible models remain namely federal leadership, legislative clarity, defined spectrum strategy, mandated participation, structured industry partnership, and measured, published performance.

ATTACHMENT C: Australian Triple Zero failures as case studies

This attachment treats the major Australian events since 2010 as case studies, in the same style as the international comparisons. Each is classified as an isolated failure (a discrete fault in one provider or component) or a systemic failure (a recurring or structural weakness), and each records the nature of the failure, the verified impact, and importantly, the ongoing implications that do not make the headlines: coronial inquests, regulatory penalties and civil litigation that follow long after the outage is restored.

1. Snapshot of major events since 2010

Date	Event / trigger	Operator(s)	Type	Verified impact
Jan 2011	Queensland floods (disaster)	Telstra / multiple	Disaster	Exchanges flooded, power lost; 000 congestion; tens of thousands lost service
3 May 2018	Pit fire + controller-card failure	Telstra	Isolated	Card failure missed among ~26,000 alarms; widespread landline 000 routing failure
2019–20	Black Summer bushfires (disaster)	Telstra/Optus/TPG	Disaster	Mass loss of mobile, ESO radio and broadcast; communities isolated
2021–22	Victorian 000 call-answer crisis	ESTA (State)	Systemic	47.4% of ambulance calls answered within 5s (Oct 2021), falling to 39% (Jan 2022)
8 Nov 2023	Software upgrade (route flood)	Optus	Systemic	2,697 failed 000 calls; 369 callers given no welfare check; ~10M offline
1 Mar 2024	CLI platform fault	Telstra	Isolated	148 of 494 calls not transferred; a Victorian man in cardiac arrest died after ambulance dispatch was delayed
18 Sep 2025	Firewall upgrade (wrong plan)	Optus	Systemic	~600+ failed 000 calls over ~13–15h; up to four deaths (2 police-confirmed)
28 Sep 2025	Regional network fault	Optus	Isolated	~5,000 customers without emergency-call access for >9 hours (Wollongong, NSW)

The 7 February 2009 Black Saturday bushfires – during which more than 18,000 Triple Zero calls went unanswered in Victoria, fall just outside the 2010 window but are the precedent that drives much of the later reform agenda.

2. Queensland floods (2011) and Black Summer bushfires (2019–20) – disaster-driven failures

Classification: disaster (physical-infrastructure and power loss). In both events the binding problem was the physical destruction of, or loss of mains power to, exchanges, towers and fibre – not the 000 routing chain itself. Communities lost mobile coverage, ESO radio and broadcast simultaneously. The lesson is that regulation cannot prevent physical destruction; better base-station backup power and operational disaster roaming would reduce, but not remove, the impact. Disaster roaming, recommended since 2020, remains in trials and is not operational – the single clearest example of a recommendation not implemented (Attachment D).

3. 8 November 2023 Optus outage – systemic failure (camp-on and welfare checks)

Classification: systemic. A software upgrade flooded routing tables and took roughly 10 million customers offline. Optus initially reported 228 failed Triple Zero calls, later revised to at least 2,697. ACMA found it had denied emergency-call access to 2,145 people and failed 369 welfare checks, and penalised Optus $12 million. The failure modes – no camp-on of 000 calls to other networks, and missed welfare checks – are precisely those the post-2023 rules were written to prevent.

Ongoing implications (sub-headline): beyond the ACMA penalty, the broader Optus reliability and data failures of 2022–2024 produced sustained litigation and consumer-redress exposure for the carrier – most prominently the Federal Court class action commenced by Slater and Gordon arising from the September 2022 Optus data breach (more than 100,000 customers registered; set down for trial commencing June 2027). While that proceeding concerns the data breach rather than the 000 outage, it illustrates the long civil-liability tail that follows carrier reliability failures long after the headlines fade.

4. 18 September 2025 Optus outage — systemic failure (detection and redundancy)

Classification: systemic. A firewall upgrade applied under the wrong change plan caused approximately 75% of more than 600 Triple Zero calls to fail across the NT, SA and far-west NSW (and WA) over about 13–15 hours; Optus's own submission to the Senate inquiry records 6,051 unique service numbers affected during the event.

The independent Schott Review (commissioned by the Optus Board, released December 2025; all 21 recommendations accepted) found that camp-on to an alternate network could take 40–60 seconds and frequently did not succeed; that the carrier's network-volume monitoring excluded Triple Zero calls, so no alarm was raised; and that emergency services and regulators were notified only after the issue was resolved. Up to four deaths were initially linked to the outage, with two later linked by police.

Detection failed before the rules did – confirmed by primary evidence. The submissions of SA Ambulance Service and South Australia Police to the Senate inquiry show that the outage was surfaced by the community and emergency services, not by the carrier's monitoring. SAAS was alerted by callers from around 11:30 on 18 September, contacted Telstra (the Emergency Call Person) at 11:35, and was told at 12:00 that there were 'no recorded outages' and that the numbers callers had used were 'not visible' on Telstra's system; SAAS then confirmed the fault itself by test-calling from Optus handsets and escalated to SAPOL. This is direct, on-the-record evidence that independent measurement – not self-report – is the only reliable basis for detection, the core of Strategic decisions 6 and 7.

Ongoing implications (sub-headline): the relevant Bean Review recommendations already existed, and the Minister publicly observed that Optus appeared not to have fully implemented them – making this as

much an implementation-and-compliance failure as a technical one, and the strongest single argument for the implementation-assurance function recommended in the submission.

5. 28 September 2025 Optus regional fault – isolated failure

Classification: isolated. A regional network fault left approximately 5,000 customers in the Wollongong area (NSW) without emergency-call access for more than nine hours. Coming days after the September 18 event, it underscores that even discrete regional faults carry life-safety consequences and that detection and notification must work at the regional as well as national level.

6. Post-3G handset incompatibility – systemic, slow-burn failure

Classification: systemic (cross-carrier, device layer). Following the 3G shutdown, certain software-incompatible 4G handsets cannot complete or camp-on for Triple Zero, and such failed attempts can be invisible to carriers. The scale of the cleanup is evident in evidence to the Senate inquiry:

- TPG reported classifying some 28,000 device models and variants, blocking around 37,000 individual phones before 1 November 2024 and a further ~7,535 that had not accepted a software update, and blacklisting nearly 13,000 model types in total;
- Samsung identified 71 older models (sold 2015–2021) still configured for emergency calling on Vodafone's former 3G network; and
- Apple shipped iOS updates (for the iPhone 12 in December 2025 and older models into January 2026) after the National Telecom Resilience Centre found those devices might fail to connect to the secondary network on a shared (MOCN) tower.

A note on the November 2025 case (the 'Wentworth Falls incident'): this incident – a TPG customer on a Samsung handset who could not reach Triple Zero – was initially reported as a death linked to an outdated device. The position was subsequently disputed: by December 2025 TPG advised it did not believe the incident involved a fatality, and Telstra's supplementary evidence records that the relevant agency had not verified the connection.

We therefore do not state it as a confirmed death; it nonetheless illustrates both the device-layer risk and the real difficulty of establishing, during and shortly after an incident, whether a failed call contributed to a death. The device and manufacturer layer remains under-addressed in the framework, with no orderly class-level mechanism – the gap that Strategic decision 5 targets.

7. 1 March 2024 Telstra CLI fault – isolated operational-discipline failure

Classification: isolated. A Calling Line Identification (CLI) platform fault on 1 March 2024 – triggered by a high volume of registrations from medical-alert IoT devices that tripped a previously unknown software fault in Telstra's CLI platform – meant that, of 494 Triple Zero calls received over about 90 minutes, 148 were not successfully transferred. Telstra's contingency process then failed because several stored emergency-service numbers were incorrect. A Victorian man in cardiac arrest died after his call was not transferred and ambulance dispatch was delayed. ACMA found 473 breaches and penalised Telstra more than $3 million (December 2024). This was an operational-discipline failure within a single provider rather than a gap in the rules – evidence that CLI and location integrity and transfer success must be measured outcomes, not assumptions.

8. Victorian 000 call-answer crisis (2021–22) – systemic capacity failure at the State layer

Classification: systemic (State call-answer layer). Between late 2021 and early 2022 ESTA – (Victoria's 000 call-taking and dispatch body) could not answer emergency calls within target. In October 2021 only 47.4% of ambulance calls were answered within five seconds against a 90% benchmark; by January 2022 the figure was 39%, with some callers waiting more than ten minutes. The Inspector-General for Emergency Management found ESTA could not provide enough call-takers because of its funding model.

Ongoing implications (sub-headline): media analysis linked call-answer delays to dozens of deaths over an 18-month period, and the Coroners Court of Victoria has examined whether delays contributed to individual deaths (for example, ongoing coronial attention to specific cases). The episode drove the IGEM review (Sept 2022, 42 findings / 8 recommendations), the Ashton Capability and Service Review (May 2022, 20 recommendations), a $333 million State funding package and the rebrand of ESTA to Triple Zero Victoria. It demonstrates that a single national service is only as resilient as its weakest jurisdictional layer, and that funding-model design is itself a reliability question.

9. The litigation and liability tail – the failures that do not make headlines

The most visible consequences of a Triple Zero failure are the outage and the immediate deaths. The durable consequences are often legal and financial, and they surface years later. Three strands are worth recording.

Regulatory penalties: ACMA enforcement now produces material penalties – Optus $12 million (2023 outage) and Telstra $3 million (March 2024 fault) – with a $30 million maximum now in force. These are an increasingly significant cost of reliability failure.

Coronial inquests: State coroners examine whether outages or call-answer delays contributed to specific deaths (Victoria's ambulance-delay matters; deaths linked to the 2025 Optus outage). Coronial findings frequently generate further, jurisdiction-specific recommendations that must themselves be tracked to implementation.

Civil litigation against infrastructure owners: liability is not confined to telecommunications carriers. Electricity network owners whose assets fail – cutting power to towers and exchanges and, with them, emergency communications – face civil claims.

The clearest documented example is the litigation against Essential Energy arising from the 2018 Tathra bushfire (NSW), where the courts granted affected landowners preliminary discovery to pursue a potential class action alleging the distributor's network caused the fire; Essential Energy contested the discovery. Bushfire-ignition and power-loss events of this kind are precisely the conditions under which Triple Zero access is lost, and the resulting litigation is part of the true, sub-headline cost of an unresilient emergency-communications system.

(We note the Tathra proceeding is framed as a bushfire-ignition matter rather than a Triple Zero outage claim; we cite it as the documented Essential Energy example of the infrastructure-failure liability tail.)

10. Boundary case – Bondi Junction (13 April 2024): what is not a Triple Zero carriage failure

For completeness and rigour, the April 2024 Bondi Junction Westfield knife attack is recorded as a boundary case. The 000 network functioned during the attack; there was no carrier outage or routing failure. The issues surfaced by the coronial inquest were operational – a late and unclear 000 call from an unattended shopping-centre CCTV control room, and questions of dispatch and coordination. Telecommunications-network measures would not have changed the outcome; the relevant levers are private-security protocols, control-room staffing and emergency-response coordination. We record it to delineate clearly what falls inside, and outside, the carriage chain this Review governs.

(This is distinct from the separate December 2025 Bondi Beach terrorist attack referenced above, the subject of a current Royal Commission.)

ATTACHMENT D: Prior reviews, inquiries and legal proceedings since 2010

This attachment provides a consolidated, jurisdiction-by-jurisdiction record of the reviews, inquiries and legal proceedings since 2010 that bear on Triple Zero, emergency communications and the resilience of the underlying networks. It covers both the Commonwealth and the States, identifies the formal recommendations of each activity, and records what has been implemented and not implemented.

1. Commonwealth reviews and inquiries

Review / inquiry	Year	Key recommendations / focus	Implementation status
RC into National Natural Disaster Arrangements (Black Summer)	2020	80 recommendations incl. disaster roaming feasibility, CSP duty to carry 000, base-station backup power, telecommunications resilience	Partial – resilience funding and a CSP-carriage focus progressed; disaster roaming NOT operational (trials only since 2023)
Regional Telecommunications Review	2022	Network resilience, backup power, coverage, disaster roaming	Partial – black-spot and resilience programs funded; coverage and roaming gaps persist
Bean Review – Optus Outage Review (2023 outage)	2024	18 recs: Triple Zero Custodian, outage-communication rules, testing regime, camp-on/fall-back, welfare checks, review of all 000 law (rec 18; this Review)	Implemented / significantly progressed – 17 of 18; rec 18 is this Review
Senate Environment & Communications References Committee (2023 outage)	2024	Enforceable communications standard, mandatory outage disclosure, domestic/disaster roaming	Partial – outage-communication rules and disclosure implemented; roaming outstanding
Schott Review — 2025 Optus outage (Board commissioned, Commonwealth relevant)	2025	21 recs on emergency-calling protocols, escalation, monitoring/ alarming, testing and governance	In progress – Optus accepted all 21; verification pending
Senate Environment & Communications References Committee – Triple Zero service outage inquiry (added)	2025-26	Causes, impacts and responses to the 18 Sep 2025 Optus outage and other outages; camp-on, roaming, whole-of-government coordination, Optus/Singtel contracts	In progress – final report to be tabled 30 June 2026 (after this Review's submissions close)
This Review – Triple Zero Legislative and Regulatory Review	2026	Whole-of-framework review (Bean rec 18); final report due by March 2027	In progress

2. State and Territory reviews and inquiries

These are frequently missed in national debate but substantially determine how reforms are realised on the ground, because call-taking, dispatch and frontline radio are State (and Territory) responsibilities.

Review / inquiry	Year	Key recommendations / focus	Implementation status
2009 Victorian Bushfires Royal Commission (VIC)	2010	Surge capacity, extreme-event warnings, better ESO handover after Black Saturday	Largely implemented over time (warnings systems, ESTA surge arrangements)
Queensland Floods Commission of Inquiry (QLD)	2012	Emergency-management coordination, warnings and communications resilience during floods	Largely implemented at State level; communications-resilience gaps recurred in later events
IGEM (VIC) Review of emergency ambulance call-answer performance	2022	42 findings, 8 recommendations; ESTA funding model, call-taker capacity, public education on when to call 000	Accepted; addressed via $333m package and Triple Zero Victoria reforms
ESTA Capability and Service Review — Ashton (VIC)	2022	20 recommendations on capability, responsiveness, governance and culture; rename/restructure	Supported in principle (all 20); $333m funding; ESTA became Triple Zero Victoria
NSW Independent Bushfire Inquiry	2020	Telecommunications and power resilience, warnings, coordination (among 76 recommendations)	Accepted by NSW; resilience measures partially implemented
NSW Flood Inquiry (O'Kane/Fuller)	2022	Disaster communications, telecommunications resilience and warnings during the 2022 NSW floods	Accepted/supported by NSW; communications-resilience actions ongoing
NSW Legislative Council Select Committee — response to 2022 major flooding	2022	Emergency response and coordination, including telecommunications and connectivity failures during floods	Recommendations to NSW Government; implementation partial
NSW Telco Authority / Public Safety Network governance	ongoing	Operation of the NSW Public Safety Network (50+ agencies, 50,000+ radio users); TEMU disaster coordination	Ongoing State capability; key channel for implementing Commonwealth outage notification rules

3. Legal proceedings and enforcement since 2010

Proceeding / action	Year	Nature	Status / outcome
ACMA v Optus –2023 outage penalty	2024	Regulatory enforcement for denial of emergency-call access (2,145 people) and 369 missed welfare checks	$12 million penalty paid
ACMA v Telstra – March 2024 fault penalty	2024	Regulatory enforcement for CLI/transfer fault (148 of 494 calls not transferred); a death occurred	$3 million+ penalty paid
Slater and Gordon v Optus – data breach class action	2023–	Federal Court class action arising from the Sept 2022 Optus data breach (100,000+ registrants)	On foot; trial set down to commence June 2027 (concerns data breach, not the 000 outage)
Essential Energy – Tathra bushfire preliminary discovery / potential class action	2018–2026	Civil litigation alleging the distributor's electricity network caused the 2018 Tathra (NSW) bushfire; preliminary discovery sought	Courts granted preliminary discovery; Essential Energy contested – example of infrastructure-failure liability tail
Coronial inquests (VIC ambulance delays; 2025 Optus-linked deaths)	2022–	State coronial examination of whether outages / call-answer delays contributed to specific deaths	Ongoing; findings may generate further jurisdiction-specific recommendations

4. The pattern, and the case for implementation assurance

Read together, the record shows a consistent dynamic: a disaster or outage exposes a weakness; an inquiry, Commonwealth or State, recommends structural and regulatory change; and the government of the day accepts the recommendations, increasingly all of them. What is inconsistent is durable, verified implementation across jurisdictions. The clearest example of a long-recommended measure not implemented is temporary disaster roaming (recommended since 2020, still in trials in 2026).

The clearest example of rules existing but not being complied with is the repeat welfare-check failure by Optus in 2025. And the State-level reviews, Victoria's IGEM and Ashton reviews above, show that reliability can fail at the call-answer layer even when the Commonwealth front-end works.

This is the evidence base for Strategic decision 12: a standing, published, periodically verified register of recommendations from all relevant Commonwealth and State reviews, inquiries and major-incident investigations, vested in the Custodian, so that reform compounds rather than being re-established after each incident.

ATTACHMENT E: Sources and references

Primary instruments and reviews

1. Terms of Reference - Triple Zero Legislative and Regulatory Review, the Hon Anika Wells MP, Minister for Communications, 17 March 2026.
2. Triple Zero Custodian, Triple Zero Legislative and Regulatory Review - Consultation Paper, May 2026, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.
3. Optus Outage Review (the Bean Review), Mr Richard Bean, final report 21 March 2024 (18 recommendations); Government response 30 April 2024.
4. Independent Review - The Triple Zero Outage at Optus: 18 September 2025 (the Schott Review), Dr Kerry Schott AO, released 18 December 2025 (21 recommendations accepted).
5. Telecommunications Legislation Amendment (Triple Zero Custodian and Emergency Calling Powers) Act 2025 (commenced 31 October 2025); Telecommunications (Emergency Call Service) Determination 2019; TCPSS Act 1999; ACMA Act 2005.
6. ACMA enforcement: 'Optus pays $12 million penalty for Triple Zero outage' (8 Nov 2024); 'Telstra pays $3 million penalty for Triple Zero outage' (Dec 2024).

International case studies (Attachment B)

7. UK Emergency Services Network: GOV.UK Emergency Services Network overview; National Audit Office, 'Progress with delivering the Emergency Services Network'; House of Commons Public Accounts Committee report on ESN; Computer Weekly and Public Technology reporting, 2024–2025 (EE/BT c. £2.22bn connectivity agreement; IBM c. £1.63bn integration; c. 20,840 sites incl. 292 Extended Area Service masts; ~£11.3bn estimate; completion 2029).
8. US FirstNet: First Responder Network Authority (firstnet.gov) press releases; AT&T newsroom (about.att.com); PR Newswire and Urgent Communications reporting, 2024–2025 (7M+ connections; ~30,000 agencies; ~2.99M sq mi coverage; +20,000 sq mi in 2024; 1,000 new sites 2024–25; 11,000+ in-building sites; ~$2bn network-evolution investment).
9. FEMA roles (Attachment B.2.1): FEMA (fema.gov) Integrated Public Alert and Warning System (IPAWS) governance and Wireless Emergency Alerts pages (1,600+ alerting authorities); Emergency Support Function #2 (Communications) Annex, National Response Framework. FirstNet Authority sits within the Department of Commerce's NTIA.
10. NEMA role (Attachment B.2.1): National Emergency Management Agency (nema.gov.au) - national leadership and coordination across the emergency-management continuum (preparedness, response, relief, recovery); established 2022 within the Home Affairs portfolio.

Australian failures and prior reviews/proceedings (Attachments C and D)

11. 2023 Optus outage: iTnews, ‘Optus finds 2,697 Triple Zero calls failed’ (23 Jan 2024); ACMA penalty release (Nov 2024).
12. Victorian 000 call-answer crisis: Inspector-General for Emergency Management (Vic), ‘Review of Victoria’s emergency ambulance call answer performance - COVID-19 pandemic-related 000 demand surge’ (3 Sep 2022).
13. ESTA Capability and Service Review (Graham Ashton, final report May 2022); Victorian Premier media release, ‘Building a Stronger Triple Zero Service for All Victorians’ ($333m package; rebrand to Triple Zero Victoria).
14. Essential Energy / Tathra bushfire litigation: Lawyerly reporting on preliminary discovery for a potential class action over the 2018 Tathra bushfire (Essential Energy contesting discovery).
15. Slater and Gordon Optus data breach class action: Slater and Gordon (slatergordon.com.au); proceeding commenced 21 April 2023, trial set down to commence June 2027.
16. Royal Commission into National Natural Disaster Arrangements (2020) recommendations; Regional Telecommunications Review (2022); NSW Telco Authority / Public Safety Network (nsw.gov.au); Triple Zero Victoria Annual Report 2024–25; Queensland Ambulance Service performance data.
17. Background on how 000 works and disaster roaming status: The Conversation (UTS), ‘How do Triple Zero calls actually work?’; Mail Community, ‘Push to implement temporary disaster roaming’ (Jan 2026).

Senate Environment and Communications References Committee - inquiry into Triple Zero service outages (parallel process)

18. Written submissions: Optus (Submission 1) and attachment; Singtel (2); Department of Infrastructure / Triple Zero Custodian (3 and supplementary 3.1); ACCAN (4); Telstra (7 and supplementary 7.1); Telecommunications Industry Ombudsman (8); NSW Telco Authority (9); National Farmers’ Federation (10); Australian Telecommunications Alliance (12); ACMA (13); Apple (26); SA Ambulance Service (27); South Australia Police (28).
19. Public-hearing opening statements and correspondence: Optus (Stephen Rue, 3 Nov 2025 and 26 Feb 2026); Singtel (John Arthur, 12 Mar 2026); TPG Telecom (İnaki Berroeta, 9 Dec 2025); Ericsson (Ludvig Landgren, 9 Dec 2025); Samsung (Eric Chou, 9 Dec 2025); Google (26 Feb 2026); NEMA (Katarina Carroll, Deputy Coordinator-General, 26 Feb 2026); Chair/Minister and ACCAN–ACMA–ATA correspondence, Nov 2025 – Apr 2026. Committee final report to be tabled 30 June 2026.

Note on evidence. Consistent with the firm’s methodology, this submission distinguishes established facts (proof) from inference and aspiration, uses only verified published figures, and flags gaps rather than estimating. Events internal to the current Australian reform cycle are stated as recorded in the Consultation Paper, the firm’s research paper and the public evidence to the Senate inquiry; international and prior-review figures are drawn from the public sources listed above. Where a reported fatality remains unverified (see Attachment C.6), it is identified as such and not stated as established.