Telstra submission to the Triple Zero Legislative and Regulatory Review

Date: 30 June 2026

CONTENTS

Executive Summary

Overview

Telstra welcomes the opportunity to contribute to the Triple Zero Legislative and Regulatory Review (the Review). Telstra is Australia's largest telecommunications provider and the Emergency Call Person (ECP) for 000 and 112 emergency calls.

Triple Zero is a **critical national safety system**. Reforms should focus on continuing to enhance the reliability and accessibility of the system. This includes modernising the framework so it can safely accommodate contemporary networks, devices, services and future access pathways while also improving accessibility by giving end users more ways to contact emergency services in different circumstances.

Future technology options include messaging, the Universal Outdoor Mobile Obligation (UOMO), automated or device-initiated communications and IP-based pathways. These options create important opportunities to strengthen Triple Zero reliability, availability and resilience while also improving accessibility by broadening the circumstances in which end users can contact emergency services. However, they also require **careful safeguards, clear eligibility settings, information quality requirements and Emergency Service Organisation (ESO) readiness**. These settings are needed so innovation strengthens, rather than fragments, the national emergency communications system.

The current framework remains too voice-centric and Carriage Service Provider (CSP)/carrier-focused to be durable for that environment. It should evolve into a **technology-neutral, modular and end-to-end system framework**. That framework should set enduring principles in the core Telecommunications (Emergency Call Service) Determination (ECSD) and allow **pathway, technology or service type specific requirements to evolve over time**. It should also allocate obligations to the **party best able to control or influence the relevant function**. The framework must recognise the **interdependence of carriers, CSPs, the ECP, device manufacturers and suppliers, ESOs, regulators and government**.

Telstra supports **practical, realistic and enforceable reforms** that strengthen reliability and public confidence while minimising regulatory process overheads, so industry and government effort can be focused on **future enhancements and the delivery of reliable service performance**. Telstra considers that the four core priorities are to **prepare the framework for new access pathways and technologies**; establish **clear role-based, end-to-end accountability** across the ecosystem from device suppliers to ESOs; use **targeted risk, testing and reporting mechanisms**; and establish the Custodian as **a trusted hub for information sharing, incident coordination and end-to-end operational visibility**.

Core Positions

1. Prepare the framework for new access pathways and technologies

Telstra recommends moving to a **technology-neutral, modular framework**. That framework should enable emergency communication pathways, technologies and communication modes to be introduced, refined, scaled, retired or transitioned over time, including through major technology lifecycle changes such as legacy network exits, new mobile generations and related device sunset arrangements. It should also allow existing pathways and technologies to evolve without remaking the core ECSD requirements for each change.

This reform is necessary to keep Triple Zero fit for purpose as networks, devices, user expectations and accessibility needs change. It should also preserve national consistency, system integrity and public confidence in a simple emergency access point. The framework should safely enable a broader range of communication options for end users. It should distinguish between primary communication modes, such as carrier grade voice, and secondary communication modes, such as messaging. Each mode should have tailored expectations for reliability, redundancy, fallback, information quality, safeguards and ESO readiness. ESO readiness, receiving capability, dispatch integration and implementation roadmaps should be addressed through appropriate **Commonwealth–State/Territory arrangements**. New pathways will only improve outcomes if they can be operationalised across the full-service chain.

- The main body of the ECSD should set **enduring principles and outcomes**, with pathway-, technology- or service type-specific detail in **schedules, codes, standards**, **guidelines or agreed protocols**.
- The framework should safely enable new communication modes and access options. These include messaging, automated in-vehicle emergency calling (eCall), application-based services, device-initiated communications, satellite-to-mobile and future IP-based pathways. This should be subject to **clear eligibility, certification, safeguard, information quality, ESO readiness and implementation mechanisms**.
- The framework should **distinguish between primary and secondary communication modes**. It should apply tailored expectations for **reliability, redundancy, fallback, information quality, safeguards and ESO readiness**. A mode should not be excluded only because it cannot deliver the same reliability, redundancy or feature set as traditional voice, where it provides **meaningful additional access for users**.
- Multiple communication modes should be recognised as contributing to **access diversity**. They can improve user choice and, where implemented safely, contribute to overall Triple Zero availability and reliability alongside, but separately from, traditional carrier and CSP network redundancy and diversity obligations.
- The **optimal future delivery models for answering Triple Zero** should be reviewed well before the **Triple Zero ECP contract expires**. The review should assess **national ECP, hybrid and decentralised options**, including whether new access modes and technology pathways should be handled natively by ECPs or ESOs with appropriate capability, or through relay or intermediary services where needed. Relevant criteria should include **reliability, availability, resilience**, public simplicity, national consistency, interoperability, ESO and ECP capability,

routing in border areas and satellite/UOMO scenarios, innovation, cost, governance, accountability and transition risk. The **optimal delivery of the 106 text-based emergency relay service** should be included in the review.

- The framework should address the requirement in section 14 of the ECSD for providers to ensure its controlled networks and controlled facilities give an end-user access to emergency call services whether or not a number is currently issued to the end-user in relation to a service. The framework should clarify section 14 of the ECSD. This was relevant for copper Public Switched Telephone Network (PSTN) and mobile services but is not applicable to future pathways and technologies, such as Short Message Service (SMS), that require an active service. The framework should not assume that newer messaging, over-the-top (OTT) or application-based pathways can operate without an active service, account, data connectivity or subscription.

2. Establish clear end-to-end accountability across the ecosystem from device suppliers to ESOs

Triple Zero should be managed as a **multi-party, end-to-end ecosystem** as outcomes now depend on the **combined performance of carriers, CSPs, device manufacturers and suppliers, the ECP, ESOs, regulators and government**. It should not be managed through a carrier/CSP/ECP-centric model and should be capable of recognising both domestic and international network participants where future pathways, such as satellite-to-mobile or UOMO-related services, rely on international satellite network operators for carriage. Accountability should also be **technology-aware and proportionate**, particularly for redundancy and diversity obligations, so expectations reflect what each participant can realistically control across core, access, device, ESO and external dependency layers.

- The framework should adopt **clear end-to-end accountability**. It should recognise that outcomes depend on the interaction of **carriers, CSPs, device manufacturers and suppliers, the ECP, ESOs, regulators and government**.

- Obligations should be allocated to the party best able to control or influence each function. The framework should not rely on legacy carrier/CSP-centric constructs. It should also avoid imposing obligations on parties that cannot deliver the relevant outcome.

- The framework should explicitly recognise the role of **device manufacturers, importers, distributors, retailers, refurbishers and other suppliers** in enabling or constraining **Triple Zero access**.

- A public-facing **Australian Communications and Media Authority (ACMA)-managed device compliance register** should be established as the **authoritative source of truth**. The register should cover device Triple Zero emergency communication capability, compliance status, support status and remediation status. It should apply to mobile handsets and **all devices intended to communicate with Triple Zero**. This includes wearables, fixed phones, automated eCall, fall detection and other connected emergency communication devices.

- The **Telecommunications Labelling Notice (TLN) regime should remain the foundation** for device compliance, but be strengthened to support **audit, enforcement, traceability, register accuracy and lifecycle compliance** across the device supply chain.

- Device obligations should extend beyond **point-of-supply compliance**. They should include **lifecycle assurance, supplier responsibility, register accuracy and visibility of unsupported or non-compliant devices**. They should also support proportionate treatment of **grey-market, refurbished or otherwise non-compliant devices**.
- The Telecommunications (Consumer Protection and Service Standards Act) (TCPSS Act) and ECSD should be amended so the ECSD can recognise device-side roles and supplier responsibilities. This should apply where device behaviour materially affects Triple Zero outcomes. Requirements should be maintained through a modular approach, including Australian Standard S042.1 and relevant schedules, codes, standards, guidelines or agreed protocols.
- Where shortcomings in device emergency calling behaviour are not adequately addressed by existing standards, the framework should provide a **clear process for raising those issues with relevant global standards bodies and international device ecosystem forums**. This should include bodies such as the **3rd Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI)** where appropriate. The process should recognise that Australia is generally too small a market for **bespoke local requirements** to be economically or technically feasible.
- ESO readiness, receiving capability, dispatch integration, operational interfaces, information sharing and implementation planning should be treated as **core dependencies**. These matters should be addressed through **Commonwealth–State/Territory arrangements**.

3. Use targeted risk, testing and reporting mechanisms

The framework should focus on the **proactive identification and management of systemic risks**. It should use targeted, proportionate mechanisms that improve real-world outcomes without creating unnecessary regulatory burden. Earlier detection can help prevent incidents. It can also support faster remediation and improve confidence in the overall system.

- Introduce **participant-level Triple Zero risk management plans** limited to each participant's role and sphere of control. Introduce a **Custodian-led end-to-end system risk management plan** to identify dependencies, common failure modes and emerging issues across the ecosystem. These plans should be aligned with, but not duplicative of, **Security of Critical Infrastructure (SOCI)** or **Telecommunications Security and Risk Management Program (TSRMP)** obligations.
- Implement carefully designed, targeted and risk-based **probe-style testing** as an objective, repeatable assurance and early-warning capability for selected high-risk pathways, locations and scenarios. Testing should include controls to avoid operational risk or excessive test traffic for the ECP or live emergency call handling environment. Any required ECP uplift should be appropriately funded.
- Apply **targeted, meaningful and practicable performance reporting**. Reporting should use a small number of clear public indicators aggregated by the Custodian. More granular

information should be provided confidentially where needed. Metrics, definitions and formats should be tested through an initial confidential reporting period before public publication.

- Ensure reporting reflects each party's **role and reasonable sphere of control**. Carrier reporting should focus on network-side factors within reasonable carrier control. External factors should be excluded or appropriately contextualised.

4. Establish the Custodian as the trusted operational hub

Telstra recommends the framework establish the Triple Zero Custodian as the **trusted operational hub for end-to-end system visibility, coordination and information sharing**. This should be supported by a central repository, secure operational dashboard and the powers, governance and safeguards needed to operate them effectively. The Custodian should remain accountable for governance, information handling and the overall operating model, while being able to procure or outsource specific operational, technical or administrative support where appropriate. This should be done while preserving clear separation from the ACMA's regulatory, compliance and enforcement role.

- Establish the Custodian as the **trusted central hub** for end-to-end operational visibility. This should be supported by a **central repository and secure operational dashboard**. Together, they should provide a single authoritative view of system status, risks, incidents, agreed communications and post-incident learning priorities.

- Use the hub model to enable **standardised, role-based information sharing** into and out of the Custodian. This should include rationalised notification obligations with objective triggers, consistent data fields and controlled onward dissemination. Information should be shared with participants who need it.

- Enable the Custodian to **convene and coordinate multi-party incidents**. This should include consistent government, industry, ESO and public communications. Participants should work from a common view of impact, status, dependencies and next steps.

- Extend the hub model to **structured post-incident reviews and learning forums**. These should normally apply to incidents and issues involving or impacting multiple parties across the ecosystem. The purpose should be to identify systemic learnings and improve **Triple Zero reliability, availability, end-to-end performance and incident response**, supported by appropriate resilience measures.

- Support those coordination and review functions through a carefully bounded **limited-use information-sharing environment**. This could draw on the National Cyber Security Coordinator model. Participants should be able to share information voluntarily and in good faith for incident learning, consequence management and system improvement. The model should still preserve clear pathways for serious non-compliance, public safety action and appropriate ACMA regulatory assessment.

- The Custodian should maintain an overarching **end-to-end Triple Zero business continuity plan**. This should complement the end-to-end risk management plan. It should provide a common whole-of-system playbook for major incidents, sustained disruptions, fallback arrangements, cross-party communications, ESO interfaces and recovery priorities.

- **The ACMA should remain the regulator and enforcement body**, including for TLN-based device supply-chain compliance. Clear, bounded referral and information-sharing pathways should be established between the ACMA and the Custodian. These should preserve the Custodian's trusted coordination role and protect the integrity of its policy development and ECP contract management functions.

---

1. Introduction

The remainder of this submission is structured by reference to the consultation questions. For each question, Telstra sets out its position, the reasoning supporting that position, and the key reform proposals needed to modernise the Triple Zero framework in a practical, technology-neutral and end-to-end way.

2. Response to Questions

Q1. What principles should guide Triple Zero regulation?

What principles should guide Triple Zero service regulation in the contemporary telecommunications environment? How should these be reflected in the legislative and regulatory framework?

Position

Telstra supports retaining the current framework's core public-interest principles. These should be updated to reflect contemporary, technology-neutral and end-to-end delivery of Triple Zero. The ECSD should remain the primary instrument for setting enduring principles and system-level outcomes. These should include free and reliable access as the core objective, supported by public simplicity, national consistency, integrity, availability, resilience and end-to-end emergency communications outcomes across the full ecosystem. Consistent with the modular framework proposed in the Q2 response, detailed pathway-, technology- or service type-specific requirements should sit below those ECSD principles. They should be placed in schedules, codes, standards, guidelines or agreed protocols.

Reasoning

The existing principles of free access, reliability and a simple national emergency entry point remain fundamental. However, the current framework is still too voice-centric and carrier/CSP-focused to provide a durable basis for the contemporary Triple Zero ecosystem. Emergency communications outcomes now depend on the combined performance of end-user devices, device suppliers, access networks, carriers, CSPs, the ECP, ESOs, regulators and government. The principles should therefore make clear that Triple Zero is an end-to-end national safety system. It is not simply a regulated call carriage obligation.

The ECSD should express the enduring principles and outcomes that apply across all access pathways. More detailed requirements should be managed through the modular structure described in the Q2 response. This would allow both existing and new access pathways, technologies and service types to evolve over time. It would avoid repeatedly reopening the core ECSD requirements. It would also reduce interpretation risk by placing practical pathway-specific detail in schedules, codes, standards, guidelines or agreed protocols. At the same time, it would preserve a clear, nationally consistent set of core principles.

Those principles should also guide how obligations are allocated. Responsibilities should sit with the party best able to control or influence the relevant function. This should include appropriate recognition of device behaviour, supplier responsibilities, network performance, ECP functions and ESO readiness. This approach supports end-to-end accountability without imposing obligations on parties that cannot practically deliver the relevant outcome.

Key reform proposals

- Retain the core public-interest principles of free access, reliability, public simplicity, national consistency, integrity and resilience.
- Expand the guiding principles to expressly recognise technology neutrality and end-to-end emergency communications outcomes. They should also recognise role-based accountability,

practical enforceability and whole-of-ecosystem arrangements that support reliability, availability and resilience.

- Use the ECSD to set enduring principles and system-level outcomes. This should include outcomes that reflect the full Triple Zero ecosystem from the user and device through to networks, the ECP and, where relevant, ESO readiness.
- Adopt the modular framework described in the Q2 response. Pathway-, technology- or service type-specific detail should be placed in ECSD schedules, codes, standards, guidelines or agreed protocols. This should avoid overly complicating the core ECSD.
- Allocate obligations according to each participant's role and reasonable sphere of control. This should include appropriate recognition of device suppliers, carriers, CSPs, the ECP, ESOs, regulators and government.

Q2. Are there barriers blocking access to the benefits of new technologies?

Are there any barriers in the current legislative and regulatory framework blocking access to the benefits of new delivery technologies which could be used to contact Triple Zero? If so, what aspects of the legislative and regulatory framework need to be amended to increase flexibility?

Position

Yes. Telstra considers that the current framework is overly rigid. It remains anchored in voice-only, carrier-controlled access pathways. This limits the introduction of new access methods and new ways of delivering emergency communications. The framework should be modularised with the ECSD setting common principles and outcomes. Detailed requirements for each pathway, technology or service type should sit in ECSD schedules or subordinate instruments. These could include industry codes, standards or agreed protocols.

Reasoning

The present framework was developed around traditional voice-based telephony. It does not adequately accommodate messaging, satellite-enabled messaging such as the Telstra Satellite SMS service[1], the proposed Universal Outdoor Mobile Obligation (UOMO) framework, eCall[2], wearable devices or application-based communications. There is an increasing expectation of broader emergency access across devices and channels. However, that broader access should only be enabled where it supports, or at least does not compromise, the reliability and integrity of Triple Zero.

A modular framework would allow existing and new pathways, technologies and service types to evolve without reopening or overcomplicating the core ECSD requirements. It would also allow obligations to be tailored to the characteristics of each pathway and to different technology lifecycle stages. Voice, messaging, real-time text, satellite-enabled mobile services, UOMO-related capabilities, automated or device-initiated communications, application-based services and future IP-based pathways will have different reliability profiles, data capabilities, device dependencies, transition risks and ESO implementation requirements.

The modular framework should also recognise that some future access pathways will depend on both domestic and international carriage arrangements. Satellite-to-mobile services, UOMO-related capabilities and future non-terrestrial network pathways may involve international satellite network operators or other non-Australian network participants in the carriage of Triple Zero communications. The framework should therefore be capable of allocating obligations to domestic carriers, CSPs and international carrier or satellite network participants according to the functions they perform and their reasonable sphere of control. This is important so that emergency communications carried over international satellite infrastructure can be supported through clear eligibility, assurance, information-sharing, routing, incident coordination and accountability arrangements.

The modular framework should be supported by a structured process for keeping relevant technical standards aligned with Triple Zero evolution. This includes Australian Standard S042.1 for mobile handsets. Standards should be able to evolve in a modular way as access pathways and technologies change. They should define pathway-specific requirements for device capability, identity, location,

---

[1] https://www.telstra.com.au/support/mobiles-devices/satellite-to-mobile

[2] eCall technology is an in-vehicle safety system that automatically contacts emergency services in the event of a serious accident

validation, fallback behaviour, software support and interoperability. This would help keep technical requirements fit for purpose without reopening the core ECSD for every technical change.

The same modular structure should also manage technology lifecycle transitions. As older network generations are retired and new generations of mobile technology are introduced, the framework should identify the relevant technology baseline, device capability requirements, transition milestones, notification obligations, testing and assurance requirements, fallback arrangements and any device sunset dates. This would allow events such as a future 4G exit or introduction of 6G to be managed through targeted technology-specific modules, rather than by reopening the core ECSD for each major transition.

The modular approach should also define core end-to-end outcomes for Triple Zero delivery. These should include successful delivery of emergency communications from the user through to the ECP and, where relevant, the receiving ESO. They should also include timely connection and transfer, prioritisation where technically feasible, reliability, availability, resilience, continuity and integrity of access. Integrity should include controls to minimise non-genuine traffic and system overload. Targeted prescription should still be used where it is needed for clarity, consistency and efficient operation, including for routing, failover, prioritisation, eligibility criteria for new access pathways, notification triggers and thresholds, reporting content, data definitions and information-sharing formats.

Key reform proposals

- Refocus the framework around a modular architecture. The ECSD should set technology-neutral principles and enduring outcomes that apply across all Triple Zero access pathways.
- Place detailed pathway-, technology- or service type-specific requirements in ECSD schedules or subordinate instruments such as industry codes, standards or agreed protocols.
- Ensure relevant technical standards are maintained and updated in a modular way, including Australian Standard S042.1 for mobile handsets. This will help them accommodate both existing and new Triple Zero access pathways, technologies and device capabilities over time.
- Use the modular structure to accommodate both existing and new pathways and technologies as they evolve over time. This should include, but are not limited to, voice, messaging, real-time text, satellite-enabled mobile services, UOMO-related capabilities, automated or device-initiated communications, app-based services and future IP-based pathways. It should also support technology lifecycle transitions, including the retirement of older network generations, the introduction of new generations such as 6G, and sunset arrangements for devices that can no longer support reliable Triple Zero access on the relevant technology baseline.
- Ensure the modular framework can accommodate access pathways involving both domestic and international carriage arrangements, including satellite-to-mobile, UOMO-related and other future non-terrestrial network pathways that may rely on international satellite network operators for carriage of Triple Zero communications.
- Ensure schedules or subordinate instruments provide sufficient pathway-, technology- and service type-specific detail to reduce interpretation and compliance ambiguity.

- Define minimum standards for new access technologies, including identity, metadata and location requirements where appropriate.
- Include appropriate guardrails for automated and device-initiated calling to manage false activations, non-genuine traffic and ESO demand.
- Ensure new access methods are only enabled where ESOs have the capability and capacity to operationalise them effectively. A clear, timely implementation roadmap should also be in place.

Q3. How should the framework balance multi-modal access with reliability and redundancy?

How should the legislative and regulatory framework balance multi-modal access to Triple Zero, when compared to reliability and redundancy?

Position

Telstra considers that the framework should preserve reliable voice access as the national baseline while enabling additional communication modes that improve accessibility for different users and circumstances. These include people with disabilities, children and young people, culturally and linguistically diverse communities and users who may be unable to communicate by voice in a particular emergency.

Supporting a broader range of communication methods would better reflect diverse user needs, capabilities and circumstances, while contributing to access diversity that can improve overall availability and reliability when implemented safely. More options can be beneficial for end users where they add reliable, operationally supportable pathways and do not fragment or undermine the core Triple Zero service.

To achieve this outcome, the framework should adopt a tiered model of access. That model should enable additional communication modes while recognising that not every mode can or should be expected to deliver the same reliability, redundancy or feature set as traditional voice access.

Reasoning

Additional access channels can extend reach, improve accessibility and provide alternative pathways where voice is unavailable, unsafe, impractical or unsuitable. However, they can also introduce complexity, new failure modes and increased ECP and ESO handling burdens. Different modes may not be able to support the same level of reliability, redundancy, prioritisation, camp-on, location capability or fallback behaviour as traditional voice calls. That difference should be recognised in the design of obligations. It should not, by itself, be a reason to exclude new modes where they provide meaningful additional access for users and can be implemented safely across the ECP and ESO service chain.

The framework should recognise that different communication modes also contribute to diversity. Messaging and other non-voice communication modes may allow some users to reach emergency services where voice is unavailable, unsafe, impractical or unsuitable. That communication diversity improves user choice and contributes to access diversity, which can enhance overall Triple Zero availability and reliability. It should be considered alongside, but not conflated with, traditional redundancy and diversity obligations imposed on carriers and CSPs for controlled networks and facilities.

Accordingly, the framework should distinguish between primary and secondary communication modes. It should apply tailored expectations for reliability, redundancy, fallback, information quality, safeguards and ESO readiness. Voice should remain the high-reliability national baseline. Additional modes should be enabled where they improve accessibility and access diversity and can support overall Triple Zero availability and reliability.

Key reform proposals

- Define primary and secondary communication modes. Apply differentiated reliability, redundancy, fallback, information quality and ESO readiness expectations that reflect the technical characteristics of each mode.
- Support the controlled introduction of new modes of communicating with Triple Zero. These include text, application-based services, device-initiated communications and future non-voice or IP-based communication modes. They should be supported where they improve accessibility and access diversity, can be implemented safely across the end-to-end service chain, and do not compromise Triple Zero reliability.
- Actively explore new communication modes that improve access for users who may be unable to communicate by voice. This includes people with disabilities, children and young people, culturally and linguistically diverse communities, and users whose emergency circumstances make voice communication unsafe or impractical. This should be subject to appropriate safeguards, information quality requirements and ESO readiness.
- Make clear that a new communication mode should not be excluded only because it cannot deliver the same reliability, redundancy or feature set as voice. This should apply where it offers meaningful additional access for users and can be supported with appropriate safeguards, information quality requirements and ESO readiness.
- Recognise that multiple communication modes also contribute to diversity. They improve user choice and access diversity, and can contribute to overall availability and reliability alongside, but separately from, traditional carrier and CSP network redundancy obligations.
- Ensure ESO readiness and end-to-end operational implications are considered before enabling new access channels nationally.

Q4. Should ACMA or the Minister determine which devices or technologies may access Triple Zero?

Should the legislative and regulatory framework allow for the ACMA, and/or the Minister, to determine which class of devices or technologies should or should not be able to reach Triple Zero, in order to safeguard the integrity of access for the system?

Position

The framework should rely primarily on certification-style mechanisms and principles-based eligibility criteria. It should not rely on case-by-case approvals of individual technologies. These mechanisms should operate as part of the modular regulatory framework proposed in the Q2 response. For new device types, the existing Telecommunications Labelling Notice (TLN) and regulatory compliance mark (RCM) frameworks should be leveraged. The TLN should specify applicable device requirements, while the RCM framework should certify conformity. The ECSD framework should be used to set rules for new technologies and access methods more generally. This should include common eligibility principles in the ECSD and pathway-, technology- or service type-specific requirements in ECSD schedules or subordinate instruments. These could include industry codes, standards, guidelines or agreed protocols. Technical and consultative determinations in this area may be most appropriately made through a process led by the ACMA. This reflects the ACMA's specialist regulatory role and ability to engage directly with industry, technical experts and other relevant stakeholders.

Reasoning

A case-by-case approval model would be too slow for a changing emergency communications environment. At the same time, uncontrolled access by new devices or technologies could undermine system integrity. The more effective approach is a structured, consultative certification or eligibility framework led by the ACMA. The Department and Minister would continue to set overarching policy direction and reform priorities.

That framework should use the right regulatory tool for the relevant issue. For new device types, the TLN should remain the primary mechanism for specifying applicable equipment requirements. The RCM framework should provide the recognised conformity and certification pathway for devices supplied in Australia. The ECSD should deal with broader technology and access-method rules. These include system integrity, reliability, identity, location, validation, information quality and safeguards against non-genuine traffic. Pathway-, technology- or service type-specific requirements should be placed in schedules or subordinate instruments under the modular architecture proposed in the Q2 response. ESO readiness, implementation planning, receiving capability and operational interfaces should be addressed separately through Commonwealth–State/Territory arrangements.

Automated eCall illustrates the need for this layered approach. Device-specific requirements should be specified and certified through the TLN and RCM frameworks where those frameworks are capable of doing so. Broader access-pathway requirements should be addressed through the ECSD modular framework and relevant subordinate instruments. These include validation, throttling, routing controls, minimum data fields and safeguards against non-genuine or accidental communications.

Key reform proposals

- Establish a structured certification or eligibility framework, led by the ACMA, for determining which classes of devices, technologies or access methods may connect to Triple Zero. The Department and Minister should set overarching policy direction and reform priorities.
- For new Triple Zero-capable device types, use the existing TLN framework to specify applicable equipment requirements. The RCM framework should be used as the recognised conformity and certification pathway for devices supplied in Australia.
- Use the ECSD framework to set rules for broader technologies and access methods. These should include common principles-based eligibility criteria such as system integrity, reliability, identity, location, validation, information quality and safeguards against non-genuine traffic.
- Address ESO readiness, implementation planning, receiving capability and operational interfaces through separate Commonwealth–State/Territory arrangements, recognising that those matters sit outside the direct operation of the ECSD.
- Consistent with the modular architecture proposed in the Q2 response, place pathway-, technology- or service type-specific requirements in ECSD schedules or subordinate instruments. These could include industry codes, standards, guidelines or agreed protocols. Requirements should reflect the technical and operational characteristics of each access pathway. They should complement, rather than duplicate, TLN and RCM device compliance requirements.
- Integrate device and technology eligibility decisions with any future device compliance register. This would make approved capability, compliance status, support status and remediation status visible to relevant participants. The compliance register is described in more detail in the Q5 response.
- For automated eCall and similar device-initiated communications, require regulated safeguards. These should include validation, throttling, routing controls and other measures needed to prevent high volumes of non-genuine, accidental or poorly validated communications from entering the live Triple Zero environment.
- Define minimum information requirements for automated or device-initiated communications. These should include source, device or vehicle identity where appropriate, caller or subscriber information where available, location, time, validation status, confidence level, callback or contact options and any pathway-specific data needed by the ECP and ESOs.

Q5. Should mobile device manufacturers be considered more centrally in the framework?

Should mobile device manufacturers be considered more centrally in the Triple Zero legislative and regulatory framework (such as under the ECS Determination)? What, if any, additional requirements should apply to mobile device manufacturers to ensure mobile devices can reliably contact Triple Zero on Australian networks?

Position

Yes. Telstra supports bringing mobile device manufacturers more explicitly into the Triple Zero legislative and regulatory framework. Devices are an integral component of the end-to-end Triple Zero ecosystem. They are now a core determinant of whether emergency communications can be successfully initiated, carried and supported on Australian networks. However, device regulation should align with international device and standards ecosystems. It should also include a clear process for escalating shortcomings in emergency calling behaviour to relevant global standards bodies where those issues are not adequately covered by existing standards.

Telstra's position is that device ecosystem assurance should become a central reform priority. Mobile handsets are the most immediate and important cohort. However, the framework should apply the same principle proportionately to any device intended to communicate with Triple Zero. This includes wearables, fixed phones, automated eCall devices, fall detection devices and other connected emergency communication devices. Device obligations should extend beyond point-of-supply compliance. They should include lifecycle assurance, supplier accountability, register accuracy and visibility of unsupported or non-compliant devices.

Reasoning

Emergency calling outcomes are increasingly determined by the combined behaviour of devices and networks. Devices can affect whether an emergency communication is attempted at all. They can also affect how a device selects or reselects networks, how it retries or falls back after failure, and whether emergency calling functionality continues to operate after software or security updates. Devices can also affect whether relevant identity, location or other information is available to the network, the ECP and ESOs.

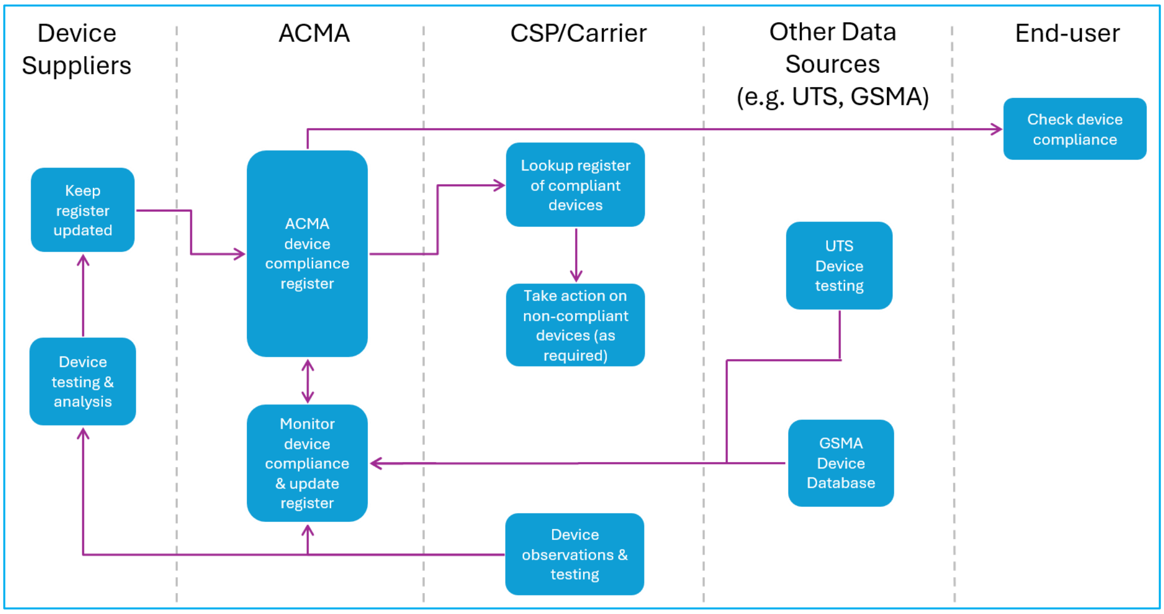
Current arrangements place disproportionate responsibility on carriers for outcomes that are materially affected by device behaviour. Carriers do not control original equipment manufacturer (OEM) design decisions, operating system behaviour, radio implementation, software updates, emergency call handling logic, network selection and reselection, fallback behaviour, location functionality or the support lifecycle for particular device models. A more integrated regulatory approach is required. Responsibility should sit with the parties best able to control or influence the supply of devices and their relevant functionality.

The current framework focuses on compliance at point of supply, with limited ongoing lifecycle assurance. That is no longer sufficient. Emergency calling capability can be affected by post-supply software updates, operating system changes, network technology evolution, changed radio capability, new voice technologies such as voice over New Radio (VoNR), emergency call handling behaviour, fallback logic, location functionality or other device-side settings outside carrier control. A device that was compliant when first supplied may later become non-compliant, unsupported or unreliable for Triple Zero access.

A public-facing device compliance register managed by the ACMA would provide the practical source of truth needed to support lifecycle assurance. Where a device model becomes non-compliant with applicable Australian emergency calling requirements, manufacturers and other responsible suppliers should identify that status on the register. This should include requirements reflected in Australian Standard S042.1 for mobile handsets. The register should clearly indicate whether a device remains compliant, is subject to remediation or software update, is no longer supported, or should not be relied on for Triple Zero access.

This register would give consumers, carriers, CSPs, retailers, refurbishers and regulators a common basis for taking proportionate action. Relevant action could include consumer notification, supply-chain controls, software remediation, withdrawal from supply, refusal to reconnect or other risk mitigation steps where appropriate. The register would also improve traceability across the device ecosystem. It would reduce the risk that unsupported, non-compliant, refurbished or grey-market devices create unmanaged risks for Triple Zero access.

The diagram below outlines the main stakeholders, and key information flows for the device compliance register.



Supplier obligations should cover the full device supply chain. Manufacturers and other responsible suppliers should be required to maintain relevant emergency calling functionality. They should also provide security and software support for a defined period, identify non-compliant or unsupported devices, and keep register information accurate over the life of the device. This should include intermediaries that specify, integrate, import, distribute, sell or place on the Australian market devices or products that are capable of directly or indirectly initiating or supporting Triple Zero communications. For example, vehicle suppliers should have appropriate responsibility for the emergency communication capability of in-vehicle eCall or other connected systems they supply, including Internet of Things (IoT) modules or embedded communications components that may trigger, support or affect emergency calling. Refurbishers should also be expressly regulated where they re-supply devices into the Australian market. This should include devices originally supplied in another market where Australian compliance marks or emergency calling requirements may not have applied. Refurbished devices should not be treated as a regulatory gap or secondary-market exception.

Australia could also consider a lifecycle support model informed by comparable international approaches, such as the European Union's ecodesign rules for smartphones, cordless phones and tablets. A comparable Australian requirement could be tailored to emergency communications. It could require manufacturers to maintain emergency calling functionality, security support and relevant software updates for a defined minimum period after the last device model is supplied in Australia. Any such obligation should be proportionate and aligned with international standards where possible. It should also be integrated with the ACMA device compliance register so unsupported or non-compliant devices are visible across the ecosystem.

While the consultation question focuses on mobile device manufacturers, Telstra's key concern is broader device-side accountability. This should apply to any device that may initiate or support a communication with Triple Zero. Mobile handsets are the most important and immediate cohort. However, wearables, fixed phones, eCall devices, fall detection devices and other connected devices should meet the same core emergency communication requirements where relevant. These include requirements relating to capability, identity, location, validation, fallback behaviour, lifecycle compliance and supplier responsibility.

These reforms should be developed consistently with the modular approach proposed in the Q2 response. Device-side requirements should sit within a broader standards architecture that can evolve as Triple Zero access pathways, technologies and device capabilities change. Technical standards such as Australian Standard S042.1 should be maintained and updated over time. They should define relevant requirements for capability, identity, location, validation, fallback behaviour, software support and interoperability. Requirements should be proportionate to the device type and access pathway.

Where shortcomings in device emergency calling behaviour are identified but are not adequately addressed by existing Australian or international standards, the framework should establish a clear process for communicating those issues to relevant global standards bodies and international device ecosystem forums. This should include bodies such as 3GPP and ETSI where appropriate. Australia is too small a market for bespoke Australian emergency calling requirements to be economically or technically feasible. The only realistic approach is to identify Australian emergency calling safety issues early. Those issues should then be articulated clearly through standards and industry channels to seek alignment with global device, operating system and chipset roadmaps.

Key reform proposals

- Introduce device lifecycle compliance obligations that extend beyond point-of-supply compliance. These should include obligations to maintain emergency calling functionality, provide relevant software and security support for a defined period, and identify devices that become non-compliant, unsupported or unreliable for Triple Zero access.
- Establish a publicly accessible device compliance register managed by the ACMA as the authoritative source of truth for Triple Zero emergency communication capability, compliance status, support status and remediation status. The register should cover mobile handsets and

any other device intended to communicate with Triple Zero. This includes wearables, fixed phones, automated eCall devices, fall detection devices and other connected emergency communication devices.

- Require manufacturers, importers, distributors, retailers, carriers or CSPs that supply Triple Zero-capable devices, refurbishers and other responsible suppliers — including intermediaries that specify, integrate, import, distribute, sell or place on the Australian market products with embedded emergency communication capability — to populate and maintain the register over the life of each device model or relevant product line. They should keep information accurate, notify relevant non-compliance or support changes, and ensure devices or embedded systems re-supplied into the Australian market meet equivalent emergency calling and technical compliance requirements.
- Apply the same core emergency communication requirements proportionately to all devices intended to communicate with Triple Zero. This should include requirements for capability, identity, location, validation, lifecycle compliance, supplier responsibility and interoperability. Requirements should be tailored to the device type and access pathway.
- Clarify the regulatory treatment of grey-market, unsupported, refurbished or otherwise non-compliant devices. This should include proportionate consumer notification, supply-chain controls, remediation, withdrawal from supply, refusal to reconnect or other risk mitigation steps where appropriate.
- Maintain and update device-side requirements through the modular standards architecture proposed in the Q2 response. This should include Australian Standard S042.1 and any relevant schedules, codes, standards, guidelines or agreed protocols. Requirements should be able to evolve as Triple Zero access pathways, technologies and device capabilities change.
- Establish a clear process for identifying and communicating shortcomings in device emergency calling behaviour that are not adequately addressed by existing Australian or international standards. Issues should be raised with relevant global standards bodies and international device ecosystem forums, including bodies such as 3GPP and ETSI where appropriate. The process should recognise that Australia is generally too small a market for bespoke requirements to be economically or technically feasible.

Q6. What outcomes should carriers, CSPs and ECPs be accountable for, and what minimum requirements are needed?

What outcomes should carriers, CSPs and ECPs be accountable for in delivering Triple Zero calls, and what minimum requirements are needed to achieve those outcomes?

Position

The framework should define clear end-to-end Triple Zero outcomes. These should be supported by role-based minimum requirements for the parts of the call path and device ecosystem that can be regulated under Commonwealth telecommunications legislation. Obligations and liability should be allocated according to the functions each party delivers and can reasonably control. Parties should not be held liable for acts or omissions of other participants upstream or downstream in the service chain. The framework should also recognise that ESOs are essential to end-to-end outcomes. ESO dependencies should be addressed through appropriate Commonwealth–State/Territory arrangements.

Those outcomes should include successful and reliable delivery of emergency communications, timely connection and transfer, prioritisation where technically feasible, availability and continuity of access, integrity of access, resilience and transparent accountability across the regulated parts of the system.

Reasoning

The current framework mixes outcomes-based and prescriptive requirements. However, it does not clearly allocate accountability across all parties that materially affect end-to-end Triple Zero outcomes. Emergency communications now depend on the interaction of devices, suppliers, access networks, carriers, CSPs, transit and routing arrangements, the ECP and ESO operational readiness. A clearer role-based model is needed. Each obligation should sit with the party best able to control or influence the relevant function.

This is particularly important in an IP and multi-party environment. Device and network behaviour together determine whether emergency communications succeed. Devices can affect call initiation, network selection and reselection, retry and fallback behaviour, software-driven emergency calling functionality, and the reliability of information provided to the network or emergency call handling environment.

Device manufacturers and suppliers should therefore not be treated only as peripheral participants regulated through the telecommunications equipment and labelling notice framework. That framework remains important, particularly at the point of supply. However, it does not fully address ongoing lifecycle issues, software-driven changes, grey-market supply, post-supply updates or the broader role devices play in end-to-end emergency communications performance. The TCPSS Act and ECSD framework should be capable of recognising device-side roles and supplier responsibilities. This should apply where device behaviour materially affects Triple Zero outcomes.

The same role-based principle applies to ESOs. Carriers, CSPs and the ECP can deliver and transfer emergency communications to the relevant termination point. However, they are dependent on ESO resourcing, systems, operational procedures, dispatch processes and jurisdictional readiness to support new access methods. Further, under the ECSD, carriers and CSPs are required to maintain network redundancy and diversity for carrying emergency calls. There is no equivalent expectation for ESOs to build complementary capability that supports end-to-end reliability, availability, and resilience across their networks and systems. If the framework is to be genuinely end-to-end, ESO dependencies need to be visible and addressed through coordinated governance. This should respect the constitutional and operational role of States and Territories.

The Commonwealth framework should recognise ESO dependencies. It should support complementary intergovernmental agreements, Memoranda of Understanding (MoUs), protocols or other arrangements. These should provide clearer expectations for ESO readiness, operational interfaces, information sharing, implementation planning and participation in whole-of-system assurance.

This is especially important for multi-modal and future access pathways. New channels will only improve outcomes if ESOs can receive the relevant communication type. ESOs must also be able to use the associated data, integrate it into dispatch workflows and respond consistently across the different State and Territory jurisdictions. ESO readiness should therefore be treated as a prerequisite for enabling new access pathways nationally. It should also be a core input into the modular framework proposed for the ECSD and related instruments.

Consistent with the modular framework described in the Q2 response, the future accountability model should define common end-to-end outcomes and minimum role-based requirements in the core framework. Detailed pathway-, technology- or service type-specific requirements should be placed in modular instruments. This would allow obligations to be tailored to the technical and operational characteristics of each pathway. It would also avoid overly complicating the core ECSD.

The same proportionality principle should apply to redundancy and diversity obligations. Section 11(2)(a) of the ECSD should be updated to reflect contemporary network realities. Full redundancy and diversity can be designed and managed more realistically in core network, critical switching, routing, signalling and platform environments than across every element of the access network. More specifically, full redundancy and diversity across the mobile radio access network, regional and remote infrastructure, customer-powered premises equipment, local access infrastructure and areas affected by power, geography, disasters or environmental constraints is not technically or economically realistic.

A better approach is to set technology-aware, role-based and proportionate expectations for redundancy and diversity as mechanisms for supporting overall Triple Zero reliability and availability. Access network obligations should focus on practical, risk-based measures, restoration capability, transparent outage management, realistic fallback arrangements and the benefits of alternative access pathways where available. The framework should also provide appropriate flexibility, exemptions or safe harbours for planned maintenance and for matters outside a party’s reasonable control.

Targeted prescription remains important where it improves clarity, consistency and operational efficiency. This is particularly the case for incident notification, reporting and performance information. Ambiguity about triggers, thresholds, definitions or required content can lead to inconsistent judgement calls, manual escalation processes and non-comparable data. Clear objective requirements in subordinate instruments, industry codes or agreed protocols would preserve the flexibility of an outcomes-led framework. They would also ensure that operational information needed to manage incidents, assess performance and maintain whole-of-system visibility is timely, consistent and usable.

Key reform proposals

- Adopt a role-based accountability model that allocates obligations to the party best able to control or influence the relevant function. The framework should not rely on CSP-centric constructs or impose obligations on parties that cannot practically deliver the outcome.
- Recognise end-user devices and suppliers as essential components of the Triple Zero ecosystem. The framework should consider how device manufacturers, importers, distributors, retailers and other relevant suppliers should be recognised under the TCPSS Act and ECSD framework where device behaviour affects emergency communications outcomes.
- Ensure any new device and supplier obligations complement the existing telecommunications equipment and labelling notice scheme, while addressing gaps that arise after point of supply or from software-driven changes in device behaviour.
- Recognise ESO expectations as essential to end-to-end outcomes. These include readiness, capability, operational interfaces, information sharing, implementation planning and the ability to receive and act on new access pathways. They should be addressed through Commonwealth–State/Territory arrangements.
- Clarify minimum operational requirements for regulated participants. These should include routing, failover, prioritisation where technically feasible, notification triggers and thresholds, reporting content, data definitions and information-sharing formats. This should be consistent with the modular framework described in the Q2 response.
- Network redundancy and diversity obligations in the future framework need to be technology-aware, proportionate and focused on what is realistic for each part of the network. Full redundancy across an access network is not technically or economically feasible. Strong reliability and resilience expectations should be maintained for core network, switching, routing, signalling and platform environments. Practical, risk-based expectations should apply to access network infrastructure, including restoration capability, outage management and fallback arrangements.
- Set realistic, measurable and enforceable performance expectations that recognise technical feasibility and contemporary IP network realities. They should also recognise multi-network call paths and the limits of each participant’s reasonable control. This includes device behaviour, radio environmental conditions, third-party failures, external power outages and other external factors.
- Provide appropriate flexibility, exemptions or safe harbours where impacts arise from reasonable planned maintenance activities undertaken to support long-term reliability, availability and resilience. Similar protections should apply where outcomes are affected by factors outside the reasonable control of the relevant party.

Q7. How should the framework support proactive identification and rectification of systemic issues?

How could the framework be amended to further provide obligations to support the proactive identification and rectification of systemic issues? What mechanisms (for example, incident learnings, mandatory improvement plans, directions, audits) are most effective, and why?

Position

Telstra supports amending the framework to improve proactive identification and management of systemic Triple Zero risks. This should be done through targeted, proportionate mechanisms. It should not create broad new regulated obligations for formal incident learning loops, mandatory improvement plans, risk-based audits or additional assurance processes. The most effective regulatory improvement mechanisms would be dedicated Triple Zero risk management plans for relevant participants. They would also include an end-to-end system risk management plan maintained by the Custodian and carefully designed probe-style testing of carrier networks from the access network through to the ECP environment.

Reasoning

Triple Zero is a dynamic, complex and distributed ecosystem. Systemic issues may emerge from the interaction of multiple parties, networks, technologies, devices and operational interfaces. A purely reactive compliance model is not sufficient for that environment. The framework should therefore support earlier identification and management of material risks before they result in incidents. It should also avoid broad, duplicative or process-heavy obligations that do not improve real-world reliability.

A dedicated Triple Zero risk management plan for each relevant participant would provide a practical mechanism for identifying risks within that participant's role and sphere of control. It would also document mitigation strategies and link material risks to ongoing operational improvement. This should apply across relevant regulated participants in the ecosystem. These include carriers, CSPs, the ECP, device suppliers and other participants whose functions materially affect end-to-end outcomes.

The Custodian should also maintain an end-to-end system risk management plan. This plan should draw on participant risk plans, relevant operational data, known incident learnings and information made available through existing reporting, engagement and coordination processes. Its purpose should be to identify dependencies, common failure modes and emerging risks. It should also identify issues that no single participant can see or manage alone.

Any Triple Zero-specific risk management plan should be a targeted emergency communications overlay. It should focus only on emergency communications outcomes. It should be limited to risks within each participant's role and sphere of control. It should avoid duplicating SOCI or TSRMP all-hazards security obligations and leverage existing TSRMP risk management artefacts where relevant. It should also align with the Custodian's whole-of-system risk view rather than creating a separate, duplicative compliance layer.

Incident learnings, feedback loops, improvement activity, audits and assurance processes can all provide useful opportunities for system learning and continuous improvement. However, Telstra does not support turning those mechanisms into new standing regulated obligations in this review. They should instead be used where appropriate through existing regulatory powers, operational governance, contractual arrangements, Custodian-led coordination, industry engagement or post-incident processes. The right pathway will depend on the nature of the issue.

Standardised probe-style testing of carrier networks used for Triple Zero calls is the second targeted mechanism that should be considered. This testing should assess whether emergency communications can traverse the regulated network path from the access network through to the ECP environment. It should use standardised test methods, definitions, termination points and reporting formats. Properly designed, this would provide an objective and repeatable early-warning capability. It would also help identify emerging network or routing issues earlier and support consistent visibility across carriers.

Probe testing should be targeted and strategic, rather than ubiquitous. It would not be realistic or proportionate to require probes to be deployed at every mobile base station, or to require the ECP to process very high volumes of test traffic from every access point. The framework should instead focus probe deployment on the highest-risk pathways, locations and scenarios. These may include representative samples of network types and geographies, remote or disaster-prone areas, known coverage or routing risk areas, new or changed access technologies, major network transition points, and other areas identified through incident learnings, risk plans or Custodian system analysis. This would provide meaningful assurance and early warning without creating unnecessary cost, operational load or risk to the live Triple Zero environment.

Probe testing must be implemented carefully so it does not create risk for the ECP or the live emergency call handling environment. Test traffic should be clearly identifiable, controlled and rate-limited where needed. It should be terminated or handled in a way that does not consume operational ECP resources or interfere with genuine emergency calls. The technical design, termination points, volumes, timing, escalation protocols and reporting requirements should be agreed with the ECP and Custodian before implementation.

This capability should also be properly funded. Establishing and operating standardised probe testing across carrier networks and the ECP environment will require technical design, systems integration, monitoring, reporting, governance and ongoing operational support. If the Review recommends this capability as a national assurance measure, the associated funding model should be resolved up front. This will help ensure implementation is sustainable and does not divert resources from existing reliability and resilience activities.

Overall, the most effective regulated mechanisms are those that improve risk visibility and early detection without creating unnecessary process obligations. Participant risk management plans would place responsibility with the party best able to manage the relevant risk. A Custodian-maintained end-to-end risk plan would identify dependencies and systemic issues that sit across the ecosystem. Probe-style testing would provide objective operational assurance of the regulated network path. Other mechanisms should remain available or be used where appropriate through existing governance and regulatory pathways. These include incident learning, improvement plans, directions, audits and broader assurance activities. They should not be established as new standing regulated requirements.

Key reform proposals

Risk management plans

- Require each relevant participant in the Triple Zero ecosystem to maintain a dedicated Triple Zero risk management plan. The plan should identify, manage and periodically review the risks within that participant's role and sphere of control.
- Require the Custodian to maintain an end-to-end system risk management plan. The plan should draw on participant plans, relevant operational data, known incident learnings and existing reporting, engagement and coordination processes. It should provide a whole-of-system view of material risks, interdependencies, common failure modes and emerging issues.
- In implementing those risk management plan requirements, the framework should make clear that any Triple Zero-specific plan complements existing risk and security obligations. It should not create a separate or duplicative compliance regime. The following design principles should therefore apply:
- Ensure any Triple Zero-specific risk management plan focuses only on emergency communications outcomes and risks within each participant's role and sphere of control.
- Avoid duplicating SOCI or TSRMP all-hazards security obligations and allow participants to leverage existing TSRMP risk management artefacts where relevant.
- Align participant risk plans with the Custodian's whole-of-system risk view rather than creating a separate, duplicative compliance layer.

Access network probe testing

- Establish standardised, targeted probe-style testing of carrier networks used for Triple Zero calls. Testing should assess the path from selected access network points through to the ECP environment. It should use agreed test methods, definitions, termination points and reporting formats.
- Require probe testing deployment to be targeted, risk-based and strategic. It should focus on the highest-risk pathways, locations and scenarios rather than requiring probes at every base station or generating excessive test traffic for the ECP or live emergency call handling environment to process.
- Design probe testing as an assurance and early-warning capability for the regulated network path, rather than as a source of operational risk for the ECP or the live emergency call handling environment.
- Ensure test traffic is clearly identifiable, controlled and rate-limited where needed. It should be terminated or handled in a way that does not consume operational ECP resources or interfere with genuine emergency calls.
- Agree the technical design, termination points, volumes, timing, escalation protocols and reporting requirements with the ECP and Custodian before implementation.
- Resolve the funding model for standardised probe testing up front. Implementation will require technical design, systems integration, monitoring, reporting, governance and ongoing operational support as Triple Zero access pathways and technologies evolve.

- Enable probe testing outputs, where feasible, to contribute to the Custodian's end-to-end operational dashboard discussed in the Q9 response. This would provide an additional data source for system health, trend analysis and early warning of possible issues.

Q8. Should new performance reporting be introduced?

Should new and ongoing performance reporting for carriers and/or CSPs providing access to Triple Zero be introduced? If yes, what metrics should be reported and how often?

Position

Telstra supports exploring a targeted performance reporting framework for Triple Zero. It must be designed to improve public confidence, support Custodian oversight and provide meaningful visibility of system reliability. It should do so without creating misleading public impressions or unnecessary regulatory burden.

Public reporting should be limited to a small number of clear and consistently measurable outcomes. Those outcomes should be understandable for the average Australian. More granular information should be provided confidentially to the Custodian where needed for system oversight, operational assurance, incident learning and trend analysis. Reporting should be aggregated and published by the Custodian. Carrier-level information should be used confidentially rather than published in raw or disaggregated form.

Any reporting framework should be role-based, technology-neutral and proportionate. Carrier reporting should focus on standardised, objectively measurable network-side performance factors within reasonable carrier control. It should exclude or appropriately contextualise factors such as device behaviour, third-party failures, disaster impacts, extended power outages, planned maintenance and other matters outside a carrier's reasonable control.

Relevant reporting proportionality considerations include overlap with existing reporting obligations (such as under the *Telecommunications (Customer Communications for Outages) Industry Standard 2024*).

Reasoning

Performance reporting can improve transparency and public confidence, but only if the reported metrics are meaningful, measurable and understandable.

Triple Zero system performance is complex and depends on multiple parties. These include networks, devices, the ECP, ESOs, regulators and government. Reporting that is too technical, too granular or insufficiently contextualised may confuse the public. It may also distort accountability or create regulatory burden without improving outcomes.

The reporting framework should therefore distinguish between public transparency and operational oversight. Public reporting should focus on a small number of aggregated indicators that explain system reliability in simple terms.[3] More detailed or sensitive information should be provided confidentially to the Custodian. This would support whole-of-system visibility, trend analysis, assurance and incident learning.

The outcomes-based obligations in sections 11 and 19 of the ECSD may provide useful starting points for reporting design. These include the proper and effective functioning of controlled networks and

---

[3] A similar approach was used in the aggregated reporting on the effectiveness of the implementation of the single European emergency number '112' – see - [EUR-Lex - 52024DC0575 - EN - EUR-Lex]

facilities used for emergency calls, and the carriage of emergency calls to the relevant termination point. Section 21, relating to prioritised transfer of calls, may also be worth considering. Existing or emerging data sources could help inform reporting against these outcomes. These include data provided under the ACMA Directions and any standardised probe-style testing capability discussed in the Q7 response.

It is important that reporting reflects each party's role and reasonable sphere of control. Carriers can report on network-side performance factors relevant to the carriage of emergency calls. They can also report on the proper and effective functioning of controlled networks and facilities used for emergency calls. However, reporting metrics should avoid attributing responsibility to carriers for outcomes materially affected by device behaviour, operating system changes, user conditions, radio environment, third-party failures, ESO readiness or other matters outside carrier control.

More specifically, reporting should avoid seeking to measure performance on the device side of the mobile air interface. Carriers do not control the radio environment experienced by individual users. This includes coverage depth, building penetration, terrain, congestion, interference, handset orientation, battery state or user location at the time of the attempted call. Nor do carriers control the emergency calling behaviour, modem implementation, operating system logic, software version, antenna performance or supported capability of each device. Most importantly, a carrier has no reliable network-side means of measuring an attempted emergency call that fails before the device attaches to, camps on, or otherwise presents signalling to the network. Reporting such attempts would therefore be incomplete, non-comparable and potentially misleading.

The reporting model should be developed carefully before public publication. An initial confidential reporting period would allow data definitions, thresholds, reporting formats and measurement methods to be tested and refined. This should include steps to ensure consistency across mobile network operators. This would help avoid premature public benchmarks based on immature or non-comparable data. Public reporting should be aggregated and published by the Custodian. Triple Zero performance is a public safety issue, not a source of competitive differentiation. This is why there are mechanisms such as camp-on in the event of individual network failure or absence. Publishing raw or disaggregated carrier-by-carrier results could create misleading comparisons. Networks differ materially in scale, topology, architecture, geography and operating conditions. Aggregated Custodian-led reporting would better support public confidence while preserving confidential access to more granular information for oversight.

Finally, any reporting framework should recognise operational realities and support innovation. No network can be made one hundred per cent reliable in all circumstances. Planned maintenance is necessary to sustain long-term reliability and availability, and to maintain the resilience needed to support those outcomes. The framework should also remain adaptable as existing and new access technologies evolve. These include satellite-enabled services, UOMO-related capabilities, automated or device-initiated communications and future IP-based pathways.

Key reform proposals

- Introduce a targeted Triple Zero performance reporting framework to improve public confidence, support Custodian oversight and provide meaningful visibility of system reliability.
- Limit public reporting to a small number of clearly defined, understandable and measurable outcomes that are meaningful to the Australian public.

- Use the Custodian as the central aggregation and publication point for public reporting, with carrier-level or more granular information provided confidentially where needed for oversight.
- Focus carrier reporting on network-side performance factors within reasonable carrier control, including matters relevant to the carriage of emergency calls and the proper and effective functioning of controlled networks and facilities used for emergency calls.
- Avoid publishing raw or disaggregated carrier-by-carrier data. This could lead to misinterpretation, inappropriate benchmarking, reputational distortion or competitive distortion.
- Develop metrics, definitions, thresholds, reporting formats and cadence through consultation, and test them through an initial confidential reporting period before public publication.
- Consider using existing or emerging data sources to support reporting against relevant ECSD outcomes. These include data provided under the ACMA Directions and any standardised probe-style testing capability. Relevant outcomes could include sections 11, 19 and 21.
- Exclude or appropriately contextualise factors outside reasonable carrier control. These include device behaviour, device capability, operating system or software behaviour, radio environmental conditions, failed access attempts that do not attach to or present signalling to the network, third-party failures, regional and remote operating conditions, disasters, extended power outages, equipment failures linked to power loss and planned maintenance.
- Build appropriate flexibility, exemptions or safe harbours into the reporting framework for planned maintenance and other matters outside the reporting party's reasonable control.
- Ensure any new reporting obligations are proportionate, including by having regard to existing overlapping obligations.
- Design the reporting framework so it remains technology-neutral, adaptable to future access technologies and supportive of innovation.

Q9. What information should be shared across industry and/or ESOs, and what governance is needed?

What information is and should be shared across industry and/or ESOs to support the proactive, reliable and future-proof delivery of Triple Zero. What governance arrangements are needed to enable timely, secure and usable information sharing?

Position

The framework should support end-to-end system visibility through a centralised information-sharing hub model. The Custodian should act as the trusted central point for collecting, aggregating, validating and disseminating relevant operational information across the Triple Zero ecosystem.

The hub model is required because the current approach risks becoming an “everyone shares everything with everyone” model. That approach can create confusion, duplication, inconsistent notifications, unclear accountability and avoidable operational burden during incidents. A Custodian-led hub would simplify information flows. It would create a single, authoritative point through which relevant information is received, triaged, interpreted and shared with the participants who need it.

The model should capture inputs from all relevant participants across the end-to-end Triple Zero ecosystem. These include device manufacturers and suppliers, carriers, CSPs and the ECP, as well as ESOs and relevant government or regulatory bodies. The Custodian should maintain the central repository of truth for system status, incident information, known risks, agreed communications and operational updates. Appropriate security, confidentiality and access controls should be preserved.

The framework should also enable the Custodian to establish and maintain a secure online Triple Zero operational dashboard. The dashboard should provide an end-to-end view of system status, outages, degradations, risks, relevant incident updates and agreed operational information. Participants should be able to access the dashboard on a controlled, role-based basis. Access should be limited to current system status and information relevant to each participant’s operational responsibilities.

Reasoning

Triple Zero is now an interdependent ecosystem. It is not a simple bilateral call-delivery chain. Successful delivery depends on the interaction of end-user devices, device suppliers, access networks, transit and routing arrangements, the ECP, ESOs, government agencies, regulators and other supporting systems. No single participant has a complete view of the system. Many important risks or incidents can only be understood by combining and correlating information from multiple parties.

Current arrangements provide only partial visibility. There is significantly greater visibility of ECP performance than of network, device, supplier, ESO or broader ecosystem conditions. Information can also be fragmented across multiple regulatory instruments, notification protocols, outage processes, reporting channels and informal operational relationships. During an incident, this can create confusion. Participants may be uncertain about who must notify whom, which version of information is authoritative, what information should be shared, and how updates should be coordinated.

A hub model would address this by establishing the Custodian as the central point for receiving, aggregating and disseminating relevant information. Participants would provide relevant information to the Custodian through standardised channels, triggers, formats and definitions. The Custodian would then maintain the consolidated system view. It would determine which participants need which information and disseminate updates in a structured and timely way. This would reduce duplication, improve consistency and avoid the operational inefficiency of multiple participants attempting to notify each other separately.

For incidents involving multiple participants, the hub should support real-time coordination. It should ensure affected carriers, CSPs, the ECP, ESOs, device or access ecosystem participants and relevant government or regulatory bodies work from a common operating picture. The Q15 response addresses the specific Custodian powers and governance mechanisms needed to convene participants. It also addresses how those powers should support coordination processes and structured post-incident reviews.

The hub model should not mean that all information is shared with all parties. Instead, it should support controlled, role-based access. ESOs should receive information needed for operational decision-making and preparedness. Industry participants should receive information needed for system coordination, incident response and operational awareness. The ACMA and relevant government bodies should receive information needed for oversight, policy, assurance and external communications. Public communications should be coordinated through appropriate channels so that messaging is clear, accurate and consistent.

The Custodian should maintain a central repository of truth for relevant Triple Zero system information. This repository should include current system status, material outages and degradations, service availability and fallback status, call routing or congestion risks, relevant device or access ecosystem information, material incident updates, systemic risk insights, planned changes that may affect Triple Zero, and agreed communications material. Maintaining this central repository would help ensure that participants work from the same information. It would also reduce the risk of inconsistent messaging and support more effective coordination with government and external stakeholders.

The hub model should capture inputs from all relevant parts of the ecosystem. Device manufacturers, importers, distributors, retailers and other suppliers may hold information about device capability, compliance, software updates, emergency calling behaviour and known device issues. Carriers and CSPs hold information about network status, outages, degradations, routing, congestion, access capability and planned changes. The ECP holds information about call handling, call transfer, operational performance and incident impacts at the emergency call handling layer. ESOs hold information about receiving capability, operational readiness, downstream impacts, welfare check outcomes and jurisdictional response considerations. Bringing these inputs together through the Custodian would provide a more complete end-to-end system view.

A secure online Triple Zero operational dashboard would be a practical mechanism for implementing the hub model. The dashboard should provide a controlled, current and authoritative view of relevant system information. It could display system status, material outages or degradations, affected access pathways, incident status, update times, key operational messages, escalation status, planned changes, relevant performance indicators and agreed information from probe-style testing or other operational assurance activities. The dashboard should support both real-time incident coordination and routine system monitoring.

The dashboard should be secure and role based. Not all participants should see the same level of detail. Access should depend on operational need, security classification, confidentiality requirements, privacy considerations and legal constraints. For example, ESOs may need near real-time operational status and impacts relevant to their jurisdiction. Carriers may need information that supports cross-network coordination or situational awareness. Regulators and government stakeholders may require broader visibility for oversight and external communications, but not necessarily all technical detail.

The dashboard should complement, not replace, urgent operational notification channels. For time-critical incidents, direct operational escalation paths will still be needed. However, the dashboard would reduce reliance on ad hoc email chains, repeated bilateral updates and inconsistent manual notifications. It would give participants a trusted place to check current status, see the latest agreed update, understand whether the issue is ongoing or resolved, and identify the next expected communication.

A centralised model would also simplify notification obligations. Rather than creating multiple overlapping obligations for every participant to notify every other participant, the framework should define clear triggers, thresholds, data fields and reporting pathways into the Custodian hub. The Custodian could then manage onward dissemination according to agreed rules and role-based access settings. This would improve timeliness and consistency while reducing operational burden during incidents.

This hub model should also be used to refine and rationalise notification obligations that have developed incrementally across multiple instruments. Those obligations should be simplified and aligned. Participants should not be required to make duplicative or inconsistent notifications through multiple channels during incidents. The framework should introduce more objective and clearly defined notification triggers based on severity, functional impact and system risk. Standardised thresholds and data fields should also be used to improve consistency, comparability and automation where appropriate.

The model should also support consistent external communications. It should ensure government, regulators, industry and ESOs are working from the same facts when preparing briefings, media lines, public updates or post-incident information. The Q15 response addresses the Custodian authority and safeguards needed to coordinate those communications in practice. It also explains how this should occur while preserving role separation from regulatory compliance and enforcement.

The information-sharing framework should be proportionate. It should focus on information that is material to operational decision-making, Triple Zero reliability and availability, incident response, system risk, future access pathways, accessibility or public communications. It should avoid excessive reporting burden or unnecessary sharing of commercially sensitive, security-sensitive or personal information. Definitions, thresholds and formats should be standardised so that information is comparable and usable across the ecosystem.

The Custodian's hub role should also support information flows from ESOs back into the national system view. Where ESOs identify operational impacts, receiving capability issues, welfare check outcomes, downstream response impacts or other relevant information, those inputs should be made available to the Custodian. This should occur in an appropriate, privacy-protective and operationally proportionate form. It would help close the feedback loop between network or call-path issues and real-world impacts.

Overall, the hub model would create a more disciplined, scalable and future-proof approach to information sharing. It would improve whole-of-system visibility, reduce confusion during incidents, simplify notification pathways, support better external communications, and provide a practical foundation for future access technologies, device ecosystem visibility and end-to-end system assurance.

Key reform proposals

- Establish the Custodian as the trusted central hub for receiving, aggregating, validating and disseminating relevant operational information across the Triple Zero ecosystem. This should replace the current tendency toward duplicative “everyone shares everything with everyone” information flows.

- Define clear, standardised information flows into the Custodian hub from all relevant participants. These include device manufacturers and suppliers, carriers, CSPs, the ECP, ESOs, the ACMA and relevant government bodies. The flows should use agreed triggers, thresholds, definitions, data fields, update cadences and formats.

- Use the Custodian as the central repository of truth for system status, material outages and degradations, service availability and fallback status. It should also cover routing or congestion risks, device and access ecosystem information, material incident updates, systemic risk insights, planned changes and agreed communications material.

- Use the Custodian hub to support authorised reconciliation of relevant subscriber and device identifiers where only partial information is available. This would help authorised participants form a more complete operational view. It should be subject to appropriate privacy, security and legal controls.

- Establish a secure online Triple Zero operational dashboard, maintained by the Custodian. The dashboard should provide a controlled end-to-end view of system status, outages, degradations, risks, incident updates and relevant operational information.

- Provide role-based dashboard access for relevant participants. ESOs, carriers, CSPs, the ECP, suppliers, the ACMA and government bodies should be able to access the information they need for operational decision-making, preparedness, incident response, oversight and external communications. Access should be subject to security, confidentiality, privacy and legal controls.

- Enable the Custodian to coordinate incidents involving multiple participants. This should include incident bridge calls or equivalent real-time coordination forums where appropriate. Information should be captured firsthand and reflected in the central repository and dashboard.

- Rationalise notification obligations across relevant instruments. The framework should define clear pathways for participants to notify the Custodian. Triggers should be objective and based on severity, functional impact and system risk. Onward dissemination should occur according to agreed rules.

- Use Custodian-held information and dashboard data to support consistent government, regulator, industry, ESO and public communications during major incidents or systemic issues.

- Ensure information sharing is proportionate and limited to material operational, reliability, availability, risk, incident response, future access pathway, accessibility and communications needs. It should avoid unnecessary sharing of commercially sensitive, security-sensitive or personal information.
- Design the hub and dashboard model to scale over time. It should be able to support existing and new access pathways, device ecosystem reforms, probe-style testing, performance reporting and future Triple Zero technologies as they evolve.

Q10. Does the single national emergency call system encourage or hinder ESO innovation?

Does the objective of the single national emergency call system encourage, or hinder, the ability for state and territory organisations to innovate in their delivery of emergency calling and dispatch services?

Position

The objective of a single national voice emergency call service both encourages and constrains innovation. It provides a baseline service that ensures all users have access to emergency services through a simple, consistent and nationally recognised entry point. However, the framework can also limit timely innovation where new access methods require coordination across all jurisdictions, ESOs, systems and operational processes. The Review should therefore initiate structured work to assess future delivery models and identify the optimal approach for the next phase of Triple Zero. That work should consider how to preserve national consistency while enabling safe innovation by States, Territories and the Commonwealth.

Reasoning

The national system provides a critical, consistent baseline. It can enable innovation by giving users and service providers a stable national entry point. However, it can also hinder innovation where centralised regulation and cross-jurisdiction dependencies limit the speed and flexibility of adopting new capabilities.

The existing voice access system provides a critical foundation for accessibility, consistency and public trust. The framework should also enable modular innovation. ESOs should have flexibility to innovate in their service delivery by layering additional capabilities above the core voice access system. These capabilities could include messaging, video and enhanced data sharing outside the core call process.

To foster innovation while maintaining national consistency, it may also be necessary to consider national standards for new access methods to Triple Zero. This would support state-level flexibility in operational systems. It would also encourage pilot programs for new approaches and establish clear pathways for scaling successful innovations nationally. Those pathways should include both funding and implementation strategies. There are several potential future models that could be considered:

- **National ECP model (current approach)** — a single nationally coordinated Emergency Call Person handling all access methods and routing. The main advantages are national consistency, a simple and familiar public entry point, less complexity and centralised operational accountability. The model also supports consistent call handling and routing rules, and common standards across jurisdictions. It enables efficient national coordination for voice calls and avoids forcing users to understand jurisdictional or technology-specific differences. The main limitations are that a single national model can be slower to adapt to new technologies. It can also constrain State and Territory experimentation. New access pathways may require all jurisdictions to move at the pace of the least-ready participant where ESO capability or operational changes are needed.
- **Hybrid model** — a national ECP for voice, with other access methods delivered or coordinated by States, Territories or the Commonwealth under nationally consistent eligibility,

interoperability and assurance settings. This preserves the trusted national voice baseline. It also allows parallel innovation for new access methods such as text, application-based services, video, enhanced data, connected alarms or future pathways. It could support pilots and scaling without disrupting the core voice service. However, it would need strong governance to avoid fragmentation, inconsistent user experiences and unclear accountability. Care would be needed for border areas. It would also be needed for UOMO or satellite-enabled pathways where earth stations may be in only a few locations and caller location is not initially known. In those scenarios, routing to the appropriate State or Territory ESO may be more complex. Roles, funding, data flows, ESO readiness, routing rules and transition arrangements would therefore need to be clearly defined.

- **Decentralised model** — greater responsibility devolved to States and Territories, including direct connection to State and Territory ESOs without a national Emergency Call Person. This may give jurisdictions greater control. It may also support closer integration with dispatch and response systems, and faster local innovation where a jurisdiction is ready to invest. However, the risks are significant. It could undermine the simplicity and consistency of the national Triple Zero service. It could also create divergent user experiences and technical standards, increase complexity for carriers and CSPs, duplicate investment, weaken national situational awareness, and make cross-border, roaming, overflow, resilience and major incident coordination harder. Those risks would be heightened in border areas. They would also be heightened for UOMO or satellite-enabled pathways where earth stations may be in only a few locations and caller location is not initially known. In those scenarios, routing to the appropriate State or Territory ESO may be more complex. Any decentralisation would require careful transition planning, national interoperability and routing rules, clear accountability and strong Commonwealth–State/Territory governance.

The future model review should also consider how new access modes and technology pathways would be operationally handled in each model. Some pathways may be capable of being handled natively by an ECP, or directly by ESOs where they have the necessary receiving capability, dispatch integration, trained personnel, information systems and operational processes. Other pathways may require a relay or intermediary service, either permanently or during transition, to translate or normalise communications, manage accessibility needs, validate information quality, reduce non-genuine traffic, support routing and ensure ESOs receive information in an operationally usable form.[4] The appropriate model is therefore likely to vary by pathway, technology, jurisdictional readiness and the maturity of ESO and ECP capability.

Each model involves trade-offs across reliability, availability, consistency, resilience, efficiency and innovation. The framework should therefore remain flexible rather than locking in a single long-term model.

[4] For example, Apple's Emergency SOS via satellite uses Globalstar satellites and Apple-trained relay centre specialists to contact emergency services on the user's behalf where local emergency services cannot directly receive the satellite text communication.

Key reform proposals

- Undertake a structured review of future Triple Zero delivery models to identify the optimal long-term approach. The review should include the national ECP model, hybrid models and more decentralised options.
- Assess each model against clear criteria. Relevant criteria should include reliability, availability, resilience, public simplicity, national consistency, interoperability, ESO readiness, implementation complexity, cost, governance, accountability, innovation potential and transition risk.
- Retain the national voice baseline in the near term while that review is undertaken, recognising the continuing value of a simple, trusted and nationally consistent entry point for the public.
- Enable carefully governed jurisdiction-led or Commonwealth-led innovation. This should only occur where the innovation remains interoperable with the national system and is supported by minimum national standards for new access technologies.
- Ensure new access methods are only enabled where ESOs have the capability and capacity to operationalise them effectively. A clear, funded and timely implementation roadmap should also be in place.
- Assess whether each new access mode or technology pathway can be handled natively by an ECP, directly by ESOs where they have the required capability, or through a relay or intermediary service where native handling is not yet feasible or operationally appropriate. This assessment should consider ESO and ECP capability, accessibility needs, information quality, routing, dispatch integration, operational burden, transition timing, funding and national consistency.
- Maintain flexibility for future structural models and avoid locking the framework into a single delivery architecture before the future model review is complete.
- Complete the future model review well before the expiry of the current ECP contract. This would allow sufficient time for consultation, decision-making, procurement, funding, legislative change and transition planning.

Q11. Is there information that should be made available to ESOs through regulation?

Is there information that carriers, CSPs, and ECPs hold which is not currently, but should be made available to ESOs through regulation to support the delivery of emergency services?

Position

Yes. ESOs should receive the information they need to prepare for, manage and learn from emergency communications impacts. However, the framework should distinguish clearly between system-level operational information and individual call-level information.

System-level information should generally flow through the Custodian hub and secure dashboard model described in the Q9 response. That model should provide ESOs with timely, role-based access to relevant information. This should include system status, outages and degradations, service availability, call-path impacts, ECP impacts, device or access pathway issues, and other material information needed for situational awareness, preparedness and whole-of-system reliability, availability and resilience.

Individual call-level information should continue to be available through established operational channels and nationally consistent processes. This should apply where the information is needed for emergency response, call-backs, welfare checks or incident reconstruction. Relevant information may include subscriber details, enhanced location information, call metadata, call time, call-back attempts, call-back method, service address details, available Standardised Mobile Service Area (SMSA) information, available tower or location details, and agreed welfare check information. Sharing should remain subject to privacy, security and operational controls.

The key reform is therefore to use clear national standards and Custodian-led information flows, rather than relying on broad bilateral obligations between every carrier, CSP, the ECP and each ESO. Those standards should specify what information is shared, when, in what format, through which channel and with what safeguards. System-level information should use the Custodian hub. Call-level information should use established operational channels.

Reasoning

ESOs need different types of information for different purposes. System-level information supports preparedness, situational awareness, incident coordination, operational continuity and whole-of-system reliability, availability and resilience. It helps ESOs understand whether an outage, degradation, access pathway issue, ECP impact or device-related issue may affect their jurisdiction. It may also affect call volumes, receiving capability or downstream response planning.

That type of information is best coordinated through the Custodian hub, repository and dashboard. A central model avoids a fragmented approach. It means each carrier, CSP or the ECP does not need to separately provide overlapping information to each ESO through different channels, formats and timeframes. It also supports consistent national definitions, role-based access, security and privacy controls, and clearer external communications during incidents.

Call-level information is different because it relates to a specific emergency communication. It is needed for operational response. ESOs and Police need clear, timely and consistent information to support call-backs, welfare checks and incident reconstruction. The framework should therefore define nationally consistent minimum information standards, formats and timeframes for individual call information. Sharing should remain lawful, secure, proportionate and operationally useful.

In the welfare check context, a consistent template or equivalent process should include key information where available. This may include the time of the call attempt, number of call-back attempts or messages, call-back attempt type, service address details, SMSA information, available location or tower details and any other agreed information needed to support referral and response. These standards should be developed with carriers, CSPs, the ECP, ESOs, Police and relevant industry bodies.

Key reform proposals

System-level information

- Provide ESOs with timely, role-based access to relevant system-level operational information through the Custodian hub and secure dashboard model described in the Q9 response.
- Avoid creating duplicative direct information-sharing obligations for system-level information where the same outcome can be achieved more effectively through the Custodian hub model proposed in the Q9 response.
- Include relevant system-level information such as system status, outages and degradations, service availability, call-path impacts, ECP impacts, device or access pathway issues, and relevant network or service information.
- Apply role-based access, security, confidentiality and privacy controls so ESOs receive the information they need without unnecessary sharing of commercially sensitive, security-sensitive or personal information.
- Use standardised definitions, triggers, data fields, formats and update timeframes so information shared with ESOs is timely, comparable and usable.

Call-level information

- Ensure individual call-level information needed for emergency response, call-backs, welfare checks and incident reconstruction continues to be available through appropriate operational channels and standardised processes.
- Define nationally consistent minimum call-level information standards. These should include subscriber details, enhanced location information, call metadata, call time, call-back attempts, call-back method, service address details, SMSA information, available tower or location details and agreed welfare check information, where available and appropriate.

Welfare checks

- Develop nationally consistent formats and timeframes for welfare check referrals to Police, in consultation with carriers, CSPs, the ECP, ESOs, Police and relevant industry bodies.

Q12. Does ACMA require additional powers and mechanisms?

Are there any additional regulatory powers and mechanisms the ACMA requires to regulate Triple Zero, especially to support a framework which is proactive and future-focused?

Position

Yes. Telstra considers that the ACMA's existing powers are broad enough in principle to regulate most aspects of the Triple Zero ecosystem. However, targeted adjustments are needed so those powers can be exercised effectively across the end-to-end ecosystem. Those adjustments should support a proactive and future-focused framework.

Specifically, the reforms addressed in the Q12 response are required to ensure the ACMA can effectively monitor, audit and enforce compliance across the device supply chain under the Telecommunications Labelling Notice (TLN) framework. They are also needed so the TCPSS Act and ECSD can recognise device-side roles and supplier responsibilities where device behaviour materially affects Triple Zero outcomes. The broader allocation of system coordination, end-to-end visibility and proactive risk identification functions between the ACMA and the Custodian is addressed in the Q13 response.

Reasoning

Effective regulation depends not only on industry obligations. It also depends on whether the regulator has the right tools to monitor and respond to risks within its regulatory remit. While the ACMA has extensive information-gathering and enforcement powers, the current framework remains largely reactive and compliance oriented. This is increasingly misaligned with a Triple Zero ecosystem in which device behaviour, supplier practices and new access pathways may materially affect emergency communications outcomes.

A key practical gap is compliance and enforcement across the device supply chain. The TLN regime should remain the foundation for telecommunications equipment compliance. However, it must be capable of effective audit, traceability, lifecycle assurance and enforcement where devices may affect emergency communications outcomes. This includes mobile handsets and other Triple Zero-capable devices.

There is also a related gap where device behaviour materially affects Triple Zero outcomes. In some cases, the ACMA may not be able to impose obligations on device manufacturers, importers, distributors, retailers, refurbishers or other suppliers outside the TLN framework, including through the ECSD. Consistent with the Q6 accountability model, the TCPSS Act should be further amended. This would allow the ECSD framework to recognise device-side roles and supplier responsibilities where needed to protect end-to-end Triple Zero outcomes.

Targeted additional ACMA powers or mechanisms may therefore be needed to verify supplier compliance and require conformity evidence. They may also be needed to audit supplier records, require accurate and current device information, compel remediation or register updates, address grey-market or otherwise non-compliant supply, and take proportionate enforcement action. These powers should apply where devices or supplier practices create risks for emergency communications.

A central device compliance register would help mitigate those risks. It would create a single authoritative source of information about whether devices supplied in Australia meet applicable

Australian standards, including emergency calling requirements. The register would improve transparency and support earlier identification of non-compliant or high-risk devices. It would also assist carriers, regulators and other participants to understand device capability, support status and behaviour across the device lifecycle. Its effectiveness would depend on the ACMA having clear and enforceable powers to require relevant suppliers to include devices in the register. The ACMA would also need powers to require suppliers to keep information accurate and current, and to address non-compliance. Without those powers, the register risks becoming incomplete or voluntary in practice.

The proposed reforms should therefore strengthen the ACMA's effectiveness through targeted and proportionate enhancements focused on the device ecosystem. They should ensure the TLN regime can be effectively audited and enforced. They should also support an ACMA-managed device compliance register, enable accurate lifecycle information from suppliers, and allow timely action where non-compliant devices or supplier practices create risks for emergency communications. Broader whole-of-system coordination issues are addressed in the Q13 response.

Key reform proposals

- Introduce an ACMA-managed device compliance register as the authoritative source of truth for Triple Zero emergency communication capability, compliance status, support status and remediation status.
- Ensure the ACMA can access structured, standardised information needed for regulatory monitoring, audit and enforcement of device supply-chain obligations. This should include information about device supply, TLN compliance, register accuracy, lifecycle updates and supplier remediation.
- Consider targeted additional ACMA powers to audit and enforce compliance across the device supply chain. These should include powers to require conformity evidence, inspect or audit supplier records, compel register updates or remediation, address grey-market or otherwise non-compliant supply, and take proportionate enforcement action against non-compliant devices or suppliers.
- Extend regulatory expectations beyond point-of-supply compliance to support lifecycle assurance. This should include software updates, support status, changes in device behaviour and supplier responsibility for maintaining accurate register information.
- Amend the TCPSS Act so the ECSD framework can recognise device-side roles and supplier responsibilities where device behaviour materially affects Triple Zero outcomes. This should complement, rather than duplicate, TLN-based device compliance requirements.

Q13. Are there barriers to ACMA addressing systemic issues, including linked infringements?

Are there barriers to the ACMA considering systemic Triple Zero issues, or linking related infringements, to ensure issues indicating broader problems are addressed appropriately? If yes, what should change?

Position

Yes. The framework should better support the identification of linked patterns and broader systemic issues. This should be done with clear role separation. The Custodian should have the primary forward-looking, end-to-end system visibility and coordination role. The ACMA should remain focused on regulatory monitoring, compliance and enforcement. Where necessary, the ACMA may play a complementary role by formally seeking information for use by the Custodian. However, the preferred model is for the Custodian to obtain forward-looking operational and system information directly through its hub, repository and dashboard functions.

Reasoning

The ACMA's role is primarily regulatory. It should be able to assess related infringements, patterns of non-compliance and enforcement issues in context. This is particularly important where individual events may indicate a broader compliance issue. Broader system coordination, end-to-end visibility, proactive risk identification and improvement functions should sit primarily with the Custodian. This is consistent with its role as a whole-of-system coordination body. It should be supported by appropriate information-sharing arrangements.

The current framework also lacks a mature, integrated model for collecting and correlating information across the full emergency communications pathway. This limits the ability to identify issues that arise across devices, networks, the ECP, ESOs and other participants. It also reduces the opportunity to refine the framework to address those issues. That end-to-end visibility should be developed through the Custodian's central hub model, repository and operational dashboard. This is the model proposed in the Q9 response. It should be preferred over creating overlapping whole-of-system coordination functions within the ACMA.

The ACMA can nevertheless play an important complementary role where information-gathering powers are needed for regulatory purposes. It may also have a role where information cannot practically be obtained by the Custodian directly. In those circumstances, the ACMA should be able to seek structured, forward-looking information. It should then provide or facilitate appropriate use of that information by the Custodian, subject to confidentiality, legal and governance safeguards.

The preferred model, however, is for the Custodian to gather operational, systemic and forward-looking information directly. This should occur through the information-sharing arrangements described in the Q9 response. It should be supported by clear participant obligations and agreed data standards. This will help ensure the Custodian can maintain a trusted coordination role. It will also allow the ACMA to retain independence as the regulator and enforcement body.

The framework should therefore avoid conflating systemic operational coordination with compliance enforcement. Linked infringements and related breaches should remain matters for the ACMA. Broader forward-looking system issues should be identified and coordinated through the Custodian. These include emerging risks, multi-party dependencies, ESO readiness and device ecosystem trends. ACMA involvement should occur where a matter becomes a compliance issue or where formal information-gathering powers are needed.

There should also be a clear pathway for the ACMA to inform the Custodian where the ACMA identifies potential systemic issues through its regulatory monitoring, information gathering or enforcement work. This should apply where those issues would be more appropriately addressed through Custodian-led guidance, policy, coordination or system improvement activity rather than regulatory action. This would allow regulatory insights to inform forward-looking system coordination. It would do so without blurring the distinction between the ACMA's enforcement role and the Custodian's operational and policy coordination role.

Key reform proposals

- Clarify that the Custodian has the primary forward-looking role in maintaining end-to-end system visibility. This should include identifying emerging systemic risks and coordinating responses across the Triple Zero ecosystem.
- Confirm that the ACMA remains the regulator. Its responsibilities should include monitoring compliance, assessing related infringements and taking enforcement action where systemic issues indicate breaches of regulatory obligations.
- Enable the ACMA, where necessary, to formally seek structured forward-looking information for use by the Custodian. This should be subject to appropriate confidentiality, legal and governance safeguards.
- Prefer direct Custodian collection of operational, systemic and forward-looking information. This should occur through the hub, repository and dashboard model described in the Q9 response. It should be supported by agreed data standards and participant information-sharing arrangements.
- Support intergovernmental arrangements to better integrate ESO readiness, operational impacts and performance information into the Custodian's whole-of-system view.
- Establish a pathway for the ACMA to inform the Custodian about potential systemic issues identified through regulatory monitoring, information gathering or enforcement activity. This should apply where those issues are best addressed through Custodian guidance, policy, coordination or system improvement rather than regulatory action.
- Establish coordinated engagement and escalation pathways for resolving multi-party issues. These pathways should preserve the distinction between Custodian-led coordination and ACMA-led enforcement.

Q14. Do recent changes effectively balance the role of ACMA and the Custodian?

Do recent changes to the TCPSS Act effectively balance the role of the ACMA as a regulator with the role of the Custodian as an entity which oversees the Triple Zero ecosystem as a whole?

Position

Recent changes establish the appropriate conceptual distinction between the ACMA as regulator and the Custodian as whole-of-system coordinator. However, that role boundary now needs to be operationalised more clearly. The ACMA should remain focused on rule-setting, regulatory monitoring, compliance and enforcement. This should include targeted TLN-based oversight of the device supply chain. The Custodian should lead forward-looking end-to-end visibility, trusted information sharing, operational coordination, policy development, ECP contract management and system improvement across the Triple Zero ecosystem.

Reasoning

The legislative framework should preserve a clear functional separation between the two roles. The ACMA should regulate within its jurisdiction. This includes monitoring compliance, using information-gathering powers and taking enforcement action where obligations are breached. The Custodian should maintain the forward-looking whole-of-system view. It should coordinate information across the ecosystem, identify emerging systemic risks and lead non-enforcement responses. These responses include policy, guidance, coordination, ECP contract management and system improvement.

Maintaining that separation is important for both regulatory integrity and trusted coordination. If the ACMA becomes the primary whole-of-system coordination body, its independence as regulator may be blurred. Participants may also be less willing to share forward-looking operational information candidly. Conversely, if the Custodian takes on enforcement-style functions, its ability to act as a trusted forum for coordination, incident learning and system improvement is likely to be weakened.

Separation is also important because the Custodian's role extends beyond operational coordination. It also includes government policy development and management of the ECP contract. Those functions should remain distinct from regulatory compliance and enforcement. This will protect their integrity, preserve confidence in policy, procurement and contract management decisions, and avoid perceived conflicts. This is particularly important where operational information is shared with the Custodian for coordination or improvement purposes.

The Custodian function is still maturing. Its role should be operationalised consistently with the hub model in the Q9 response, the systemic-issues model in the Q13 response and the powers-and-operating-model response in the Q15 response. This includes aggregating information, maintaining a central repository, operating an end-to-end dashboard, identifying systemic issues, supporting policy development and managing the ECP contract.

Clear referral and escalation pathways are needed where issues move between the two roles. The ACMA should be able to inform the Custodian about systemic issues better addressed through Custodian policy, guidance, coordination or system improvement. Conversely, the Custodian should be able to refer potential non-compliance to the ACMA through clear, bounded criteria. The operating safeguards for those pathways, including limited-use information sharing, are addressed in the Q15 response.

Where formal information-gathering powers are needed, the ACMA may play a complementary role. It may seek structured information for Custodian use, subject to confidentiality, legal and governance safeguards. However, the preferred model should be for the Custodian to gather forward-looking operational and system information directly. This should occur through the Q9 hub, repository and dashboard. It should be supported by the practical powers and safeguards discussed in the Q15 response.

A trusted information-sharing model is needed to preserve this role separation. At a high level, information shared with the Custodian for operational coordination, incident learning, consequence management, policy development, ECP contract management or system improvement should not automatically become an enforcement trigger. The Q15 response addresses the detailed limited-use safeguards and operating model for that approach.

The framework should therefore avoid duplication, gaps and perceived conflicts by making the boundary clear. The ACMA should lead compliance and enforcement. The Custodian should lead forward-looking system visibility, trusted information sharing, operational coordination, policy development, ECP contract management and system improvement. Both bodies should operate through defined referral and escalation pathways where an issue has both operational and compliance dimensions.

In practical terms, this means clarifying the boundary between the ACMA's regulatory role and the Custodian's coordination, policy and contract management roles. It also means establishing formal referral pathways in both directions. Operational learning, policy development, ECP contract management and regulatory compliance pathways should remain appropriately separate.

Key reform proposals

- Clarify in legislation, instruments or supporting governance arrangements that the ACMA's regulatory, compliance and enforcement functions are distinct from the Custodian's forward-looking system coordination, trusted information-sharing, visibility, improvement, policy development and ECP contract management functions.
- Confirm that the ACMA remains responsible for rule-setting, regulatory monitoring, compliance and enforcement, including targeted device supply-chain compliance under the TLN regime where relevant.
- Confirm that the Custodian is responsible for forward-looking end-to-end visibility, proactive risk identification, trusted information sharing, incident coordination, the central repository, the operational dashboard, policy development and ECP contract management. These functions should remain separate from regulatory compliance and enforcement.
- Establish formal referral and escalation pathways between the ACMA and the Custodian. This should include pathways for the ACMA to inform the Custodian about systemic issues best addressed through Custodian policy, guidance, coordination or system improvement. Any Custodian referral of potential non-compliance to the ACMA should occur only through clear, bounded criteria.

- Require a trusted information-sharing model that preserves role separation. Detailed operating safeguards and limited-use protections should be developed as part of the Custodian powers and operating model described in the Q15 response.
- Enable the ACMA, where necessary, to use formal information-gathering powers to obtain structured information for Custodian use. This should be subject to confidentiality, legal and governance safeguards. It should also preserve the preferred model of direct Custodian collection through the Q9 hub and dashboard.
- Establish periodic reviews of the ACMA/Custodian operating model to ensure the balance remains effective as the Custodian function matures and the Triple Zero ecosystem evolves.

Q15. Does the Custodian have all powers needed to fulfil its functions?

Does the Triple Zero Custodian have all the powers needed to fulfil its functions under the TCPSS Act?

Position

The current framework provides a solid foundation for the Custodian. However, its functions should be operationalised further so it can act effectively as the forward-looking, end-to-end system coordinator for Triple Zero. The Q14 response explains the role boundary between the ACMA and the Custodian. The reforms addressed in the Q15 response should focus on the powers, resourcing, governance mechanisms and safeguards needed for the Custodian to operate the Q9 hub, repository and secure dashboard model. They should also enable the Custodian to convene participants, support incident learning, maintain whole-of-system risk and continuity arrangements, and protect trusted information sharing.

Reasoning

The increasing complexity and interdependence of the Triple Zero ecosystem requires the Custodian to have practical authority to perform the trusted coordination role described in the Q9 response. Consistent with the role separation set out in the Q14 response, those powers should not confer enforcement functions on the Custodian. They should also not blur the ACMA's regulatory role.

The Review should confirm that the Custodian has the authority, resourcing and governance arrangements needed to operate the hub, repository and secure dashboard arrangements described in the Q9 response. This includes the ability to obtain, aggregate and use relevant operational and system information from the participants identified in the Q9 response. It also includes the ability to maintain the central repository and secure dashboard, and use those tools for operational awareness, incident response, system learning, reliability, availability and resilience.

The Custodian should also have the functions needed to use Q9 information sources for proactive risk identification, early coordination and a holistic understanding of performance across the call path. This should include integrating information from participant risk plans and the Custodian-maintained end-to-end system risk management plan discussed in the Q7 response. It should also include probe-style testing, performance reporting, incident notifications, ESO inputs and other relevant operational sources.

The Custodian should also maintain an overarching end-to-end Triple Zero business continuity plan as part of its operational hub role. That plan should complement the end-to-end system risk management plan described in the Q7 response. It could build on concepts similar to the existing Triple Zero disruption protocol currently managed by the ECP. However, it should cover the wider ecosystem, including carriers, CSPs, the ECP, ESOs, device and access pathway dependencies, government communications and cross-party continuity arrangements.

The business continuity plan should identify critical dependencies, continuity roles, escalation triggers, fallback arrangements, cross-party communications, ESO interfaces, public messaging pathways and recovery priorities for major incidents or sustained disruptions. It should complement participant-level risk management and continuity arrangements, rather than replacing them. Its purpose should be to provide the common whole-of-system playbook for coordination when a disruption affects, or may affect, more than one part of the Triple Zero ecosystem.

Operationalising the Custodian's role should not involve creating enforcement powers. Instead, the framework should provide practical tools, protocols and safeguards that allow the Custodian to coordinate incidents, facilitate learning, support system improvement and use operational information appropriately. This should preserve the Q14 separation from ACMA compliance and enforcement.

This should not prevent the Custodian from procuring or outsourcing support for specific operational, technical or administrative elements of those functions, provided the Custodian remains accountable for governance, information handling and the overall operating model.

The framework should also establish practical referral protocols and bounded escalation criteria to give effect to the role-separation model described in the Q14 response. These should allow the ACMA to inform the Custodian about systemic issues better addressed through policy, guidance, coordination or system improvement. They should also allow the Custodian to refer potential non-compliance to the ACMA only where clear criteria are met. Relevant criteria could include serious or persistent potential non-compliance, unresolved public safety risk, misleading or incomplete information, failure to participate in agreed remediation, or another public interest reason for regulatory assessment.

In designing the Custodian's operating powers and safeguards, the framework could draw on the approach used for national cyber security incident coordination. A central coordinator can convene participants, maintain situational awareness, coordinate significant incidents, support consistent government communications and facilitate trusted information sharing. It can do this without displacing the separate statutory roles of regulators or operational agencies. Applied to Triple Zero, that model would support the Custodian's practical operating role while preserving the ACMA's distinct regulatory and enforcement functions.

The same model should extend beyond live incident coordination to structured post-incident reviews and other learning forums convened by the Custodian. This should particularly apply where an incident involves or impacts multiple parties across the Triple Zero ecosystem. Triple Zero incidents can involve complex interactions across networks, devices, the ECP, ESOs, operational processes, public communications and government decision-making. Participants need a trusted environment in which they can share operational facts, near misses, uncertainty, decision points, lessons learned and possible improvement actions candidly. Every disclosure should not be treated as an immediate enforcement trigger. This would improve the quality of post-incident analysis, support faster remediation and help identify reliability, availability, resilience, end-to-end performance and incident response improvements across the ecosystem.

To support that operating model, the framework should consider a carefully bounded limited-use information-sharing environment. It should apply to Custodian-led incident coordination, post-incident reviews, learning forums, consequence management and system improvement. Information shared voluntarily and in good faith for those purposes should not automatically become an enforcement trigger. The model should not provide blanket immunity, prevent appropriate regulatory action or shield misconduct. It should preserve clear pathways for serious non-compliance, enforcement referrals, public safety action and other public interest exceptions, with appropriate confidentiality, privacy and security safeguards.

Key reform proposals

- Operationalise the Custodian as the forward-looking, end-to-end system coordinator for Triple Zero. It should have the authority, resourcing and governance mechanisms needed to operate the hub, repository and secure dashboard model in the Q9 response. This may include procuring or outsourcing support for specific operational, technical or administrative elements, provided the Custodian remains accountable for governance, information handling and the overall operating model. This should not create enforcement powers that duplicate or blur the ACMA's regulatory role.

- Enable the Custodian to obtain, aggregate, validate, synthesise and use relevant operational and system information from the participants identified in the Q9 response. This should support operational awareness, incident response, system learning, reliability, availability, resilience and whole-of-system improvement.
- Use the Custodian's Q9 hub, repository and dashboard as the common operating infrastructure. It should support proactive risk identification, early coordination, incident coordination, system status visibility, performance trend analysis and whole-of-system learning.
- Require the Custodian, as part of its operational hub role, to maintain an overarching end-to-end Triple Zero business continuity plan. The plan should complement the end-to-end system risk management plan described in the Q7 response. It should provide a common whole-of-system playbook for major incidents, sustained disruptions, fallback arrangements, cross-party communications, ESO interfaces, public messaging pathways and recovery priorities.
- Enable the Custodian to coordinate multi-participant incidents. This should include incident bridge calls or equivalent real-time coordination forums where appropriate. Enable the Custodian to convene structured post-incident reviews, lessons-learned forums and other multi-party improvement forums. These should normally apply to incidents involving or impacting multiple parties in the Triple Zero ecosystem. They should support free and frank sharing of operational information, identify systemic learnings, and improve Triple Zero reliability, availability, resilience, end-to-end performance and incident response across the ecosystem.
- Develop a carefully bounded limited-use information-sharing model for Custodian-led incident coordination, incident reviews and learning forums. This could draw on the National Cyber Security Coordinator model. Information shared voluntarily and in good faith for incident learning, consequence management and system improvement should be protected from inappropriate secondary use. The model should still preserve clear pathways for serious non-compliance, enforcement referrals, public safety action and other public interest exceptions.
- Establish practical referral protocols and bounded escalation criteria to implement the role-separation model described in the Q14 response. This should include ACMA-to-Custodian referrals for systemic issues better addressed through policy, guidance, coordination or system improvement. Custodian-to-ACMA referrals should occur only where defined non-compliance, public safety or public interest thresholds are met.
- Support structured sharing of appropriate information with government stakeholders and, where appropriate, public communications to maintain trust and transparency.

- Review the Custodian's operating model periodically as the function matures and the Triple Zero ecosystem evolves. This should include changes as new access pathways, device reforms, probe testing and performance reporting are introduced.

3. Other Matters

3.1 Commonwealth–State/Territory coordination

Issue

Triple Zero operates across a federated model. The Commonwealth regulates telecommunications and the national emergency call service. States and Territories remain responsible for ESOs, dispatch systems and emergency response. This creates an important implementation gap. The Commonwealth can regulate carriers, CSPs, the ECP and relevant device-side participants. However, it cannot by itself ensure ESO readiness, operational interfaces, downstream response capability or jurisdictional consistency. A genuinely end-to-end Triple Zero framework therefore needs stronger Commonwealth–State/Territory coordination arrangements. Those arrangements should make ESO dependencies visible and accountable.

This is particularly important as Triple Zero evolves beyond traditional voice access. New pathways such as messaging, satellite-enabled mobile services, application-based services, automated or device-initiated communications and future IP-based pathways will only improve outcomes if they are reliable, operationally supportable and able to be received and acted on by ESOs. ESOs must also be able to use associated data, integrate it into dispatch workflows and respond consistently across jurisdictions. Commonwealth reform should therefore be matched by intergovernmental agreements, Memoranda of Understanding (MoUs), operational protocols or equivalent arrangements. Those arrangements should address ESO readiness, implementation planning, testing, information sharing, funding, public communications and participation in whole-of-system assurance.

Key reform proposals

- Establish stronger Commonwealth–State/Territory coordination mechanisms. These could include intergovernmental agreements, MoUs, operational protocols or implementation frameworks. They should support end-to-end Triple Zero outcomes while respecting State and Territory responsibility for ESOs and emergency response.
- Better recognise ESO readiness, receiving capability, dispatch integration, operational interfaces, downstream response impacts and resilience as essential dependencies in overall Triple Zero reliability, availability and system performance.
- Ensure reforms involving new access methods are supported by clear jurisdictional readiness assessments, implementation roadmaps, testing arrangements, information-sharing rules, funding decisions and nationally consistent operational protocols. These should be in place before those methods are enabled at scale.

3.2 Access to Triple Zero without an active service

Issue

Section 14 of the ECSD requires a carriage service provider to ensure that its controlled networks and controlled facilities give an end-user access to emergency call services. This applies whether or not a number is currently issued to the end-user in relation to a service. The note to section 14 also makes clear that this requirement applies even if a relevant controlled network or controlled facility is owned or operated by a carrier. In that case, carriers are required to assist providers under section 8.

However, section 14 was developed for legacy voice contexts. In those contexts, access without an active service or currently issued number could be technically supported, particularly for copper PSTN and mobile voice emergency calling. It does not translate neatly to newer access methods. Those methods may depend on active provisioning, customer-powered equipment, device or service configuration, an account, data connectivity or an active subscription. This is particularly relevant for future messaging, over-the-top (OTT) and other application-based pathways to Triple Zero. Those pathways generally require the device or user to have an active service, account or data connectivity. This differs from current mobile voice emergency calls.

National Broadband Network (NBN) voice illustrates the issue. Voice access may depend on an active NBN service, powered customer premises equipment, network termination equipment, modem configuration or service provisioning. Where that is the case, the access-without-active-service obligation cannot operate in the same way as legacy PSTN or mobile voice access. The framework should therefore clarify that section 14 is technology dependent. It should apply only where the relevant controlled networks and controlled facilities can technically support that form of access.

The same principle should apply to unused legacy copper PSTN lines. The framework should clarify that soft dial tone does not need to be maintained indefinitely for lines that have not been in use for a material period, such as 12 months. This should apply where there are no future plans for those lines to be used for PSTN access. Maintaining soft dial tone in those circumstances is unlikely to improve real-world access to Triple Zero. It may also impose unnecessary operational and maintenance burden on legacy infrastructure.

Key reform proposals

- Clarify section 14 so the obligation remains outcomes-based and technology-aware. It should apply only where access without an active service or currently issued number can be technically supported by the relevant controlled networks and controlled facilities.
- Clarify that section 14 should not be applied to newer access methods in a way that assumes Triple Zero access can be provided without an active service. This should apply where access depends on active provisioning, customer-powered equipment, network termination equipment, modem configuration, device or service configuration, an account, data connectivity or an active subscription.
- Clarify that soft dial tone obligations do not require CSPs or carriers to maintain unused legacy copper PSTN lines indefinitely. This should apply where the line has not been in use for a material period, such as 12 months, and there are no future plans for the line to be used for PSTN access.

- Avoid imposing obligations that cannot be satisfied by particular technologies or architectures. This includes where access depends on an active service, issued number, customer-powered equipment, device capability, service configuration, data connectivity or other factors outside the reasonable control of the CSP or carrier.
