

OPTUS

Submission to Triple Zero
Custodian

**Triple Zero Legislative and
Regulatory Review**

June 2026

Public

CONTENTS

Executive Summary	3
Legislative principles for access	6
Interdependency of mobile devices and networks	19
Industry obligations	25
Reporting.....	29
The legislative framework impact on ESOs	33
Regulatory oversight of Triple Zero	36

EXECUTIVE SUMMARY

Optus welcomes the opportunity to provide a submission to the Triple Zero Custodian's Triple Zero Legislative and Regulatory Review. Triple Zero is a critical service in Australia's telecommunications ecosystem and Optus takes its obligations in relation to emergency call delivery seriously.

This submission reflects Optus's ongoing commitment to a Triple Zero framework that is reliable, resilient and fit for the contemporary telecommunications environment while ensuring that any changes to that framework are proportionate, evidence-based, practical and allocated to the parties best placed to fulfil them. Optus supports the submission from the Australian Telecommunications Alliance (ATA).

The framework needs to evolve, but carefully

The existing legislative and regulatory framework was designed for a world that uses fixed-line voice or circuit switched mobile voice. Mobile devices now account for the overwhelming majority of Triple Zero calls, and an expanding range of technologies (including wearables, connected vehicles, LEOSat direct-to-device services) are raising important questions about whether this framework is still fit-for-purpose.

Optus supports modernising the framework to reflect this reality. However, the public safety function of Triple Zero means this should be done in a thoughtful and methodical way. Expanding the framework to incorporate new access modes should only be done after systemic, end-to-end testing across all call delivery aspects – including device, networks, ECP and ESO systems – and after detailed consideration of any requirements that should apply to alternate access modes.

There may be clear and demonstrable benefits to regulating a new access mode or technology which justifies a departure from the currently accepted requirements of contacting emergency services, and which outweigh any risk of eroding public confidence in, or the reliability of, access to emergency services. In such a circumstance, it would be additionally important that the public understands and appreciates the role which in any complementary access mode plays within the broader emergency access regulatory infrastructure.

A clear statement of principles should underpin the framework

Optus recommends that the review establish a clear statement of principles in the TCPSS Act and the ECS Determination to provide a durable foundation for the framework as it evolves. Key principles Optus proposes include: reliability and redundancy as the foundation of any access mode; technological neutrality in obligations but not in outcomes; ESO readiness as a prerequisite before new access modes are introduced; proportionate accountability across the entire supply chain; flexibility with appropriate safeguards; accessibility for all end-users; and transparency and long-term financial sustainability of the ecosystem.

Accountability must be distributed across the whole supply chain

A Triple Zero mobile call currently traverses multiple parties — from a device, across a network and the ECP carrier network before intersecting with the ECP and ultimately finishing with emergency services organisations (ESOs)— each of which is a potential point of failure. The current framework concentrates accountability on MNOs and at the ECP end, leaving significant gaps elsewhere.

Optus recommends that the framework expressly allocate accountability where key elements contribute to an emergency call's success, such as device configuration. Accountability across the supply chain is also a critical consideration when introducing any new access modes, such as direct to device (D2D) calls using satellite networks. Mobile network operators (MNOs) should not be accountable for aspects of the call path or network elements they do not control.

A current gap exists in relation to device manufacturers, who sit largely outside the primary Triple Zero legislative framework. The supplier Declaration of Conformity (**SDoC**) and *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2025 (TLN)* regime require a Regulatory Compliance Mark (RCM) at point of sale, but imposes no ongoing obligations on manufacturers if devices subsequently lose emergency calling capability nor does it apply to devices purchased from overseas. This is a design flaw that Part 4 of the ECS Determination has partially addressed by placing the burden of identification and blocking on MNOs, but it does not address the root cause. Optus supports bringing device manufacturers directly into the framework and the establishment of an independent, publicly accessible device register to assist industry and better inform consumer purchasing decisions.

The review presents an opportunity to consider the respective roles of government agencies and industry in delivering coordinated education and communication about the ECS and any potential new access methods or technologies, including their capabilities, limitations and appropriate use of such alternate pathways. Greater clarity regarding responsibility for public communications and stakeholder engagement during ECS disruptions would also be welcome. Responsibilities for public education, consumer awareness and communications during incidents should be clear and assigned to the parties best placed to fulfil those functions.

Reporting and transparency for the emergency call path

Optus supports increased transparency over critical aspects of emergency calls. Recent information provided by MNOs to the Triple Zero Custodian is providing increased visibility of key metrics. A publicly accessible device register would improve transparency about device capability – even confirming if device capability is unknown or untested can assist industry and users.

Optus also supports extending reporting obligations to the emergency call person (ECP) which is currently accountable only through a commercial contract with the government that is not publicly transparent. Given that the ECP is funded through industry levies and per-call interconnect charges ultimately borne by carriers and end-users, greater transparency over the ECP's costs, performance and funding arrangements is essential.

On the broader question of interconnect charges, Optus notes that there is currently no regulated rate controlling what the ECP may charge carriers per call to Triple Zero. Optus considers that as the review considers expanding MNO obligations — including testing, reporting and potentially new access mode requirements — the funding model must also be examined to ensure it remains fair, efficient and transparent.

Clarity in oversight roles is critical

The Bean Review¹ resulted in significant changes to the ECS Determination in late 2024 and 2025. The Triple Zero Custodian has been operational since October 2025. A post-implementation review of these changes is anticipated and Optus considers this is the right sequencing. The case for expanding ACMA's powers or the Custodian's functions has not yet been made — any expansion should require clear evidence of a specific function that cannot be performed using existing measures.

The most pressing structural issue concerning the ACMA and Triple Zero Custodian is not one of inadequate powers but of coordination between the two oversight bodies. Without clear delineation of roles, industry risk receiving conflicting guidance or inconsistent requests from two separate entities on the same subject matter. Optus recommends that ACMA and the Triple Zero Custodian enter into a Memorandum of Understanding that clearly defines their respective responsibilities.

Ongoing engagement is welcome

Optus appreciates the Triple Zero Custodian's indication this is the first consultation step in this comprehensive review. Given the broad range of issues canvassed and fundamental questions about the legislative and regulatory framework we look forward to further ongoing engagement as these matters are worked through — particularly where more detailed policy discussion about the Triple Zero ecosystem may be necessary.

¹ Mr Richard Bean, Review into the Optus outage of 8 November 2023 – Final Report, March 2024. Available at: https://www.infrastructure.gov.au/sites/default/files/documents/review_into_the_optus_outage_of_8_november.pdf

LEGISLATIVE PRINCIPLES FOR ACCESS

Introduction

The current legislative and regulatory framework for Triple Zero was developed in the 1990s, primarily to support access via fixed-line voice calls. While the framework has been progressively updated, the fundamental architecture and the assumptions underlying it, continue to reflect an era of voice telephony before mobile devices became the dominant access method. Today, around 78% of Triple Zero calls originate from mobile devices,² and a growing range of technologies — from wearables and connected vehicles to low earth orbit satellite (LEOSat) services — are raising questions about their role in the Triple Zero ecosystem and its framework.

This section sets out Optus's views on the principles that should guide regulation of the Triple Zero service, the extent to which the current framework presents barriers to new technologies, and how the framework should balance innovation against the reliability and redundancy that are fundamental to a public-safety service.

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

The current principles framework

Existing principles and objectives underpinning emergency call service regulation are set out across two levels:

- TCPSS Act section 147(2), which sets the objectives the ACMA must have regard to when making (and also when amending) the ECS Determination. These objectives focus significantly on the substance and mechanisms by which emergency calls are expected to be carried.
- ECS Determination section 5(2), which contains more principles-based objectives including 'ensuring the highest levels of access, integrity and service continuity' of emergency calls is maintained.

While these existing purpose and objective provisions have served the development of the emergency calling system and ECS Determination well to date, there is a gap in the current principles underpinning emergency calling and the broader questions that the framework now faces (such as how to evaluate new and emerging technologies and access modes against the integrity and reliability imperative, or how to allocate responsibility across a multi-party supply chain).

² <https://www.triplezero.gov.au/triple-zero/How-to-Call-000/advanced-mobile-location>

In this context, Optus considers there is scope to further expand on these provisions with a clear statement of principles underpinning the Triple Zero legislative and regulatory framework holistically. This would ensure consistency in making any subordinate regulation and in the exercise of powers by the ACMA, Triple Zero Custodian or any other decision makers.

Proposed additional principles

Optus proposes the following principles to guide Triple Zero regulation in the contemporary environment:

Reliability and redundancy as the foundation

Any framework should continue to treat reliable voice connectivity as the foundation of Triple Zero. Alternative access modes and technologies should be assessed against whether they enhance or risk compromising reliability and redundancy. Some access modes may more appropriately be treated as complements to traditional voice calls if they have technical limitations in comparison. Regulatory obligations should take this into account and not assume equivalence where it does not exist.

Technological neutrality in obligations, not in outcomes

The framework should specify what must be achieved rather than how it must be achieved. This avoids locking in prescriptive operational obligations that may not be future-proof; for example, where alternative access modes are considered in future. Outcomes-based obligations allow industry to adapt to technological change without requiring primary legislation each time.

ESO readiness as a prerequisite

New access modes should not be brought into the framework with regulatory obligations attached if ESOs and the ECP are not able to effectively accommodate those modes. The cost and complexity of adapting ESO systems (which are state and territory government responsibilities) should not be underestimated, and Commonwealth regulation should not impose network-level obligations on carriers ahead of confirmed ESO capability.

Proportionate accountability across the supply chain

Obligations should fall on the party best placed to fulfil them and be proportionate to the risks being addressed. This encompasses all parties relevant to emergency call success — device manufacturers, MNOs, CSPs and the ECP — and each party should be accountable for their specific segment, not for outcomes that depend on decisions made by others in the chain. This should also include any parties related to future access modes, such as LEOSat D2D service providers.

Flexibility with appropriate safeguards

The framework should enable decision makers to respond quickly to emerging technologies or identified risks without requiring new or amended primary legislation each time. This

flexibility should be balanced with industry consultation and procedural fairness requirements, given the complex operational nature of emergency call delivery and the potential consequences of poorly calibrated interventions.

Accessible for all end-users

The framework should continue to ensure that accessing the emergency call service is available for all Australians, including those with disabilities. Calls should remain free to end-users, and access for those who rely on the National Relay Service or other accessibility pathways should be preserved and strengthened as technology evolves.

Transparency and long-term financial sustainability

The framework should require transparency of the ECP's performance, costs and funding arrangements. This would assist in determining whether the current funding model (based on a combination of government funding and industry contributions) is efficient, whether the ECP is recovering more than its actual costs, and whether interconnection charges imposed on other carriers are reasonable and cost reflective. As MNOs and CSPs face increasing obligations including mandatory testing, reporting and potential new access mode obligations, any expansion of those obligations must be considered in the context of the overall funding and charging arrangements, to ensure the framework is financially sustainable and equitable across all contributing parties.

Reflecting principles in the legislative and regulatory framework

Optus considers that these principles should be embedded in the framework at multiple levels to give them enduring legal force and interpretive weight:

- reflecting the principles in the Telecommunications Consumer Protection and Service Standards (TCPSS) Act (under section 147(2) or similar) would require that the ACMA have direct regard to these principles when considering amendments to the ECS Determination; and
- reflecting the principles within the ECS Determination would ensure that these principles form part of any interpretation of the obligations of parties subject to the ECS Determination.

The most effective mechanism would be to incorporate a clear objects clause or statement of principles into the TCPSS Act, as the enabling legislation for the ECS Determination. The TCPSS Act is the foundation of the Triple Zero framework, and a principles-based objects clause in the Act would cascade through all subordinate instruments, and ensure that as the ECS Determination is amended over time to address new access modes, new technologies or new obligations, each amendment is assessed against and anchored in a consistent set of principles.

The ECS Determination should then be amended to incorporate a complementary purpose or objects clause that reflects and gives effect to the TCPSS Act principles at the instrument

level. This would ensure that the provisions of the ECS Determination (and the obligations of parties therein) are considered in the context of these principles, providing a consistent interpretative lens for the ACMA, the Triple Zero Custodian and the courts.

For specific principles that require ongoing regulatory action (such as those related to transparency and financial sustainability), more targeted mechanisms will also be needed. This could include an obligation on the ECP to publish audited performance and cost data, a requirement for the ACMA or ACCC to assess whether interconnection charges are cost-reflective, and a mechanism for reviewing government funding arrangements in line with the ECP's evolving cost base. These mechanisms could be established through amendments to the ECS Determination or via a separate instrument, without requiring changes to primary legislation.

Post implementation reviews

Optus strongly supports post-implementation reviews for new and changed regulations to determine whether there are any amendments that could make the regulations more effective. We have appreciated the ACMA's willingness to engage with industry in relation to such reviews. We would welcome further review of the Telecommunications (Customer Communications for Outages) Standard and recent amendments to the ECS Determination regarding outage notifications, given the prescriptive operational requirements. It may be beneficial to examine:

- (a) if the requirements are achieving their intended objectives,
- (b) if outcomes can still be achieved while streamlining operational requirements,
- (c) if there is consistency in interpreting definitions.

2. 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?

The gap in the Triple Zero framework

The issue is not that the current legislative and regulatory framework creates explicit barriers that block new delivery technologies, but rather that the framework was constructed contemplating access only via traditionally delivered voice calls. The concept of an 'emergency call service' (defined in the Telecommunications Act but used widely across the Triple Zero regulatory framework) is inherently framed around a call or voice-based service; likewise, the concept of an 'emergency telephone service' in the ECS Determination is defined as a standard telephone service (STS) or a public mobile telecommunications service (PMTS).

A consequence of this is that emerging access modes and technologies which do not meet the requirement of being a call or voice-based service (e.g. SMS), or which are not traditional STS or PMTS based voice services (e.g. D2D), are not neatly addressed by the existing framework. While they are not prevented from allowing access to emergency services, they are also not regulated to the same extent (if at all), for example, in relation to reliability and redundancy.

Increasing flexibility in the regulatory framework

As matters stand, there is no clear legislative pathway through which an alternative access mode or technology that is not a voice service (or an STS/PMTS) can be formally recognised and regulated under the ECS Determination short of introducing or amending primary legislation. The current framework (especially the ECS Determination) establishes standards of access to emergency services which, even when removed from a specific voice-services context, can be reduced to certain fundamental principles. Examples of these include reliability and availability standards, redundancy, priority in carriage, minimisation of non-genuine contacts, free to access, and conveyance of location information.

Later in this submission (at Question 3) we consider whether certain access modes and technologies are presently appropriate for regulating under the Triple Zero framework.

Increasing flexibility in the framework could be achieved by:

- (a) Amending primary legislation (such as the Telecommunications Act and TCPSS Act) to establish a core set of emergency service access principles and requirements which are access / technology neutral.
- (b) Replacing existing references in primary legislation with technologically neutral provisions to accommodate new access modes and technologies.
- (c) Specifying any access mode-specific conditions or requirements in subordinate regulatory instrument/s (e.g. ACMA or Ministerial direction/determination or standard, such as the ECS Determination).

Such changes would allow new access modes / technologies to be introduced into and operate within the ecosystem (but without requiring it) subject to appropriate conditions or access mode-specific requirements (see our response to Question 4 for more information)

This approach would:

- (a) preserve flexibility for the framework to evolve with technology, while ensuring that any new obligations are subject to proper consultation and assessment before they take effect.
- (b) maintain voice calls as the primary emergency service contact method, while creating a pathway for alternative modes to be regulated once they are recognised as having reached sufficient technical and operational maturity to meet the core principles already established in the current ECS framework.

Any such changes to the Triple Zero framework will likely require detailed consultation and policy discussion with Triple Zero ecosystem participants (including emergency service organisations, the National Emergency Communications Working Group (NECWG), Triple Zero Custodian, platform providers, consumer groups and other key stakeholders).

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

Overarching approach

As noted in the consultation paper, there are several alternative pathways for contacting Triple Zero or otherwise contacting ESOs for emergency assistance, many of which are already present in the Australian market. These include SMS, LEOSat D2D, Connected vehicles (eCall), fall-detection and wearable devices, and video-calls.

Consistent with our response to Question 2, there is scope to amend the Triple Zero framework to allow pathways for such new access modes and technology types, subject to these meeting the underlying principles of access to emergency services.

Current assessment of specific access modes

There are benefits to having multi-modal access to Triple Zero and to emergency services generally. However, before new access mode or technology type are incorporated:

- (a) The new access modes must be thoroughly understood in terms of capability and functionality as compared with the STS and PMTS.
- (b) The full telecommunications ecosystem – spanning networks, devices, the ECP, and state and territory ESOs – must be demonstrably ready to support any new access mode end-to-end, reliably, and at scale.

Some of the capability considerations for these emerging access modes that go to reliability and redundancy are set out below.

SMS

The technical limitations of SMS are fundamental and unlikely to be overcome in a way that would provide the same reliability as voice calls. SMS is inherently a store-and-forward protocol; as a result, delivery does not have the same real time or guarantee characteristics as voice calls, and short messages cannot be prioritised in the way that emergency calls currently are. SMS also does not present Calling Line Identification in a way that triggers an IPND lookup with the same reliability as a voice call, creating location identification challenges (noting precise location information is fundamental to emergency calling and public safety) – potentially necessitating the exchange of multiple SMS to ensure the correct information is conveyed to ESOs.

SMS could potentially be considered as a complement to voice calls (and a supplement to the National Relay Service) in specific accessibility contexts, but whether its technical

limitations mean it can meet consumer expectations of an emergency call access method should be subject to significant further investigation before any regulatory change is made.

LEOSat D2D

D2D services are still at a very early stage in terms of use and availability in Australia, and do not currently meet the technical requirements of STS or PMTS calls for emergency call purposes. The specific technical gaps include:³

- (a) **Current SMS capability only:** The current LEOSat constellation scale and technology is only demonstrating the initial capability of supporting SMS messaging, and is not yet capable of supporting voice calls nor data-centric services.
- (b) **Location accuracy and availability:** location determination for D2D satellite services currently relies on Cell-ID or coarse network positioning methods which are not aligned with industry Advanced Mobile Location requirements,⁴ and which can provide accuracy measured in the tens or hundreds of kilometres, rendering it extremely impractical for emergency response in many scenarios. Precise caller location is fundamental for effective emergency services, yet GPS-assisted location via satellite D2D has not been validated across the consumer device ecosystem.
- (c) **Call continuity and handover between networks:** Call continuity while on the move, both within the LEO Sat D2D coverage areas, and between terrestrial mobile network and LEO Sat D2D network. Seamless mobility handover is important for emergency calls and two-way communications while on the move, however has not yet been defined or tested.
- (d) **Emergency camp-on:** A fundamental failsafe requirement of access to the emergency call service is the requirement that devices accessing the terrestrial mobile network allow access to alternative mobile networks when the home network is unavailable (commonly referred to as 'camp-on').⁵ It is not clear if this function can be supported with a D2D service, as Triple Zero routing requirements under host-network outage scenarios have not been demonstrated or validated in real-world conditions.

³ These issues are further detailed in Optus' submission to the Senate Inquiry: Optus, *Submission in response to Environment and Communications Legislation Committee Inquiry: Telecommunications Legislation Amendment (Universal Outdoor Mobile Obligation) Bill 2025 (Public Version)*, dated April 2026.

⁴ See the 'most precise location information available' in the ECS Determination, and Industry Guideline G557.6:2021 (*Advanced Mobile Location*).

⁵ This function is most commonly referred to as 'camp-on' publicly and in the consultation paper, however there is a distinction between 'camping-on' when a device is in a limited service state (i.e. not connected to its home network, roaming on another network, or SIM not present/blocked) and 'retry and reselect' processes which occur when the device is in a normal state but there is a failure in the network component causing the emergency call to retry and reselect on the home network and then across other available networks.

- (e) **Priority handling and pre-emption:** Emergency calls must receive network priority over general traffic to ensure completion during periods of congestion,⁶ which is achieved across terrestrial networks using established prioritisation and pre-emption protocols. Currently there are no equivalent capacity management and prioritisation protocols for D2D satellite services between satellite constellation operators, meaning there is no existing basis on which to guarantee emergency calls carried over D2D will be carried with priority.
- (f) **Congestion management during mass emergency events:** Unlike terrestrial networks with established congestion management and emergency services network prioritisation, D2D satellite handling of mass calling events remains untested. A disaster event generating simultaneous emergency calls from a concentrated geographic area may saturate the relevant satellite beam capacity, with no established mechanism for managing that congestion in the D2D context.
- (g) **Interoperability with ESOs:** Effective emergency call service delivery requires end-to-end integration across a complex chain of systems and organisations (see Question 6 below for more detail on this chain of systems). In the D2D context, integration with Triple Zero call-handling infrastructure, emergency service routing protocols (ESRP), location-based routing to appropriate Public Safety Answering Points (PSAPs), and callback capabilities all require validation across D2D satellite architectures.
- (h) **Call establishment reliability and latency:** D2D satellite services face inherent latency constraints arising from orbital altitude, as well as intermittent connectivity driven by satellite constellation pass timing. Emergency call establishment time and completion reliability under real-world conditions (considering factors including atmospheric interference, terrain obstruction, and satellite availability windows) have not been comprehensively tested. Until systematic testing has been completed and validated, there is no guarantee that D2D services can reliably satisfy the performance thresholds that an emergency call obligation requires under the current Triple Zero framework.
- (i) **Callback and two-way communication continuity:** Emergency call scenarios frequently require callbacks to disconnected callers, and sustained two-way communication for medical guidance and situational updates. D2D satellite service continuity during extended calls or callback scenarios has not been verified, and may be materially constrained by satellite pass duration and handover reliability between satellites. Where a call drops due to a satellite passing out of range and continuity of service is not maintained (and callback is not guaranteed), the consequences in an emergency context are potentially serious – particularly given the above-noted location information limitations.

⁶ See for instance, section 21 of the ECS Determination.

These technical gaps demonstrate a fundamental gap in the current D2D service technology and the reliability and redundancy expectations of Triple Zero regulation applied against traditional voice access.

In addition, there is a structural gap present in Triple Zero legislative framework in the context of regulation of D2D services and emergency calls. The ECS Determination regulates emergency calls in relation to carriers' (or CSPs indirectly through support from carriers) controlled networks and controlled facilities. Whereas under a D2D model, a material component of that network infrastructure is controlled by satellite operators (many of whom are large international companies). This results in a structural gap between where the regulatory responsibility sits and the entity with operational control over the network infrastructure.

While access to and use of D2D services is likely to see significant increase over coming years (particularly with the proposed UOMO obligation), noting these technical limitations, at present D2D may better be considered as a complement or addition to existing emergency voice calls rather than as a separate access mode, at least until such time as these limitations can be overcome and D2D emergency calling possesses the same qualities of redundancy and reliability as required under the current framework.

Connected vehicles (eCall)

The non-genuine call risk for connected vehicles is real and significant — minor impacts, vehicle theft alerts, or test-mode activations can generate high volumes of calls to Triple Zero. Optus understands that some vehicle emergency call systems currently route contacts through a manufacturer or third-party response centre before connecting to the ECP, which provides some filtering of non-genuine contacts. However, this arrangement is not consistent across all manufacturers and is not currently regulated. The regulatory responsibilities across the automotive supply chain, between vehicle manufacturers, embedded SIM providers and MNOs, also require clarification before connected vehicle emergency calling is more formally incorporated into the framework.

Fall-detection and wearable devices

Wearable devices present similar concerns to connected vehicles in relation to non-genuine calls. Even leading consumer devices are well documented as generating false positives; for example, triggering emergency contacts during sport or other physical activity. Increasing the burden of non-genuine calls on the ECP could materially undermine the reliability of the system for genuine callers.

It is also not clear that wearables are currently captured by existing technical standards such as the TLN, creating a regulatory gap for devices that are already in market and contacting emergency services. 'Smartwatches' and 'personal alert devices' are also excluded from the scope of Part 4 of the ECS Determination, with the effect that wearables are not subject to

the same requirements as other mobile devices requiring them to be properly configured to carry emergency calls on home and other available networks.

Video calls

Video calls require significantly greater bandwidth than voice calls and could increase network congestion, particularly during natural disasters or other major emergency events when networks may already be under pressure. This presents network management challenges that would need to be resolved before video access to Triple Zero could be considered.

It is also worth noting that support across the ecosystem on 3GPP standards-based video calls, such as Video call over LTE (ViLTE), has not gained traction, and the options that can be leveraged may be over-the-top (OTT) solutions (e.g. FaceTime, WhatsApp) that may also suffer reliability concerns. Building on the model used by the NSW Police Force BluLink service (where video is initiated by police after a voice call is connected, rather than originating as a Triple Zero call type) may be a more practical approach that avoids adding to MNO network obligations at this stage.

Considerations for introducing multi-modal access

Optus recommends that, before any new access mode or technology is recognised under the ECS Determination or otherwise incorporated into the regulatory framework, there is a systemic process in place to:

1. confirm that the new access mode or technology can meet the currently accepted core capabilities of a reliable emergency contact service;
2. confirm that the ECP and ESOs across all states and territories have the capability to receive and respond to contacts via the relevant mode or technology without degrading performance or reliability; and
3. ensure clear allocation of obligations across all key stakeholders in the supply chain for each access method/technology.

Such a process must involve end-to-end testing of the new access mode or technology at scale to identify its capabilities and limitations, and consultation with industry, community and other relevant stakeholders.

Where an access mode or technology cannot meet the same core capabilities derived from the existing framework around emergency voice calls, there may be scope for considering whether:

- such new access mode or technology could be regulated as a complement to existing emergency call services rather than an additional (substitute) access method; or

- mode-specific or technology-specific regulatory obligations — lower in some respects, stricter in others — could be implemented via subordinate regulation to address specific concerns outcomes appropriate to that technology.

In either case the overarching expectation should be that any new access mode or technology does not erode the reliability and redundancy of, and therefore public trust in, the function of emergency services contact in Australia.

Further consideration should also be given to the management of non-genuine calls particularly if there is a chance these could increase with certain access modes. While obligations currently sit with MNOs, MNOs have no visibility over the content of a call and are limited in the steps that can be taken to minimise non-genuine calls. MNOs may be able to focus on technical connectivity issues (for example related to device registration), but, are limited in what they could do where a device incorrectly calls emergency services (for example, false-positive emergency calls associated with smartphone fall/crash detection, or connected vehicles eCalling theft detection). It is likely that the ECP may be better placed to manage whether such calls are genuine.

Therefore, the framework should have the flexibility and capability to address specific concerns related to additional access modes, such as:

- (a) The management of non-genuine calls (e.g. for connected vehicles and wearable devices), and
- (b) The allocation of obligations across the delivery path where different parties control network infrastructure (e.g. for LEOSat D2D calls where significant portions of the network applicable to a D2D service are owned by potential non-MNO entities outside of Australia).

4. 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?

Existing powers of the ACMA and Minister are broad

Under the existing telecommunications legislative framework, the ACMA (and the Minister) have broad powers to introduce amendments and variations to Triple Zero related regulations, including across both the ECS Determination and related Industry Standards:

- (a) Section 147 of the TCPSS Act requires that the ACMA make a written determination in relation to emergency call services – this is the legislative basis for the ECS Determination. Section 147(7) specifies the ECS Determination as a legislative instrument, thereby empowering the ACMA to similarly amend or revoke the ECS Determination.⁷ While this is a broad power, it is somewhat limited by the

⁷ By virtue of section 33 of the *Legislation Act 2003* (Cth).

requirements of ss.147(9)-(9A) which require the ACMA to consult industry/stakeholders as well as the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, prior to amending the ECS Determination.

- (b) Section 14 of the *Australian Communications and Media Authority Act 2005* (Cth) (ACMA Act) empowers the Minister to give written directions to the ACMA in relation to the performance of the ACMA's functions and the exercise of the ACMA's powers. This power has been used to direct the ACMA to introduce amendments to the ECS Determination in the past.⁸
- (c) The Minister can also issue written directions under section 125AA of the Telco Act to the ACMA to determine an industry standard, which can broadly relate to participants in the telecommunications industry and matters relating to telecommunications activities.
- (d) The ACMA also has the indirect ability to determine an industry standard if the ACMA considers an existing industry code is deficient and has complied with the requirements of section 125 of the Telco Act.

Additional powers available to the ACMA as a telecommunications regulator are discussed in our response to Question 12.

The above powers are relatively broad and allow the ACMA the flexibility to consider and consult upon amendments to the ECS Determination, as well as allowing the Minister to direct the ACMA to amend the ECS Determination / Industry Standards, to better address emergency call services and related principles.

This would suggest that no additional powers are needed for the Minister or ACMA to determine which class of devices or technologies should or should not be able to reach Triple Zero.

Guardrails in exercising powers should remain

While we do not currently foresee the need for any additional powers for the ACMA/Minister, recognising that such powers could become desirable following further consultation, we do consider there are some general guardrails appropriate to how such powers might operate in the context of determining whether device classes or access modes can access emergency services. For instance, any such power should only be exercised to make or amend obligations where there is a clear and prescient need for intervention, to

⁸ For instance, the Minister issued the *Australian Communications and Media Authority (Emergency Call Service Determination) Direction 2024* under section 14 of the ACMA Act, pursuant to which the ACMA introduced the *Telecommunications (Emergency Call Service) Amendment Determination 2024 (No. 1)* which introduced significant amendments to the ECS Determination.

address some new development or risk which has emerged in the context of the Triple Zero framework or related emergency calling infrastructure.

Similarly, any such power should not extend to making determinations or an assessment of whether individual device models or types are able to, or are not able to, access emergency services / Triple Zero. It is not appropriate for the ACMA/Minister to be explicitly approving (or rejecting) particular device models for use/sale in Australia, as this would amount to a de facto pre-market approval regime, which would create significant regulatory burden for device manufacturers and could impede legitimate innovation. Consistent with the current regulatory regime, whether an individual device is capable of access to emergency services within the applicable regulatory framework should be left to technical standards and labelling requirements (i.e. if an individual device model meets these requirements then they are approved). Relevant to this discussion, we note our submissions in response to Question 5; in particular:

- (a) The proposed mobile device register, which operates more as a record of compliant devices providing information against which the public can consider their device choices and which can inform MNO device blocking activities under the ECS Determination.
- (b) The proposal to introduce dynamic compliance regulation of devices as they are updated and evolve over time, rather than focusing on static compliance at the time of supply to the market.

Likewise, while the current ECS Determination amendment powers under the TCPSS Act section 147 require prior industry, stakeholder and Department consultation, this is an important and necessary control given the operational complexity of emergency service access and delivery, and the potential for unintended consequences, which we would not support removing (whether in the section 147 context or more broadly for related powers to amend).

INTERDEPENDENCY OF MOBILE DEVICES AND NETWORKS

5. 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?

The existing framework focuses on Australian point of sale

The capabilities and configuration of devices are a critical element to the successful delivery of an emergency call, yet device manufacturers currently sit largely outside the main Triple Zero legislative and regulatory framework. Manufacturer obligations for all mobile devices with telephony functions are confined to a point-of-supply compliance regime under the *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2025* (TLN) and the associated technical standard *Telecommunications (Mobile Equipment Air Interface) Technical Standard 2022* and the industry code *AS/CA S042.1:2022 – Requirements for connection to an air interface of a Telecommunications Network, Part 1: General (AS/CA S042.1)*.

Mobile devices sold via Australian retailers must comply with the TLN and hold a Regulatory Compliance Mark (RCM), which requires a supplier Declaration of Conformity (SDoC) attesting that the device meets applicable Australian technical standards, including AS/CA S042.1. Only devices with the RCM should be supplied in Australia. However, devices purchased overseas or from international retail sites (like marketplace sites), otherwise known as grey imports, may not have an Australian RCM and therefore, may not meet Australian technical standards.

However, the RCM certification process typically covers basic Triple Zero call scenarios at the time of supply. There is no regulatory process to enforce or audit ongoing obligations on manufacturers to ensure devices continue to meet those standards if functionality subsequently changes (for example, due to network changes or software/firmware changes of the device).

Device configuration is important for emergency calls

Recent events have illustrated this gap clearly. Part 4 of the ECS Determination, introduced in October 2024, requires CSPs to identify devices that are not configured to be able to access Triple Zero either via the provider's own mobile network or by camping on to an alternative available mobile network, and to block those devices where such configuration issues are identified.

Whether a particular mobile phone is or is not configured to be able to access Triple Zero under these conditions can depend on a wide variety of factors, related to the manner in which a particular device configuration interacts with an underlying mobile network. Significantly, the underlying mobile network in question is relatively static (in the sense that

there are a defined number of available mobile networks in Australia), and while networks are constantly evolving, they typically do so in well-documented and well-publicised ways over significant periods of time (e.g. decommissioning a generation of mobile technology, or general network upgrade rollouts). Conversely, at any given time there may be thousands of different mobile device models (bought in Australia or overseas) connected to that network, each of which may interact differently with the same network depending on various factors, such as their operating system, software version, country of origin and/or provisioning.

Obligations do not currently apply to the right party

The ECS Determination is focussed on remediation by MNOs/CSPs in the post-identification context after a device issue is detected. The ECS Determination, which carries the primary requirements and obligations for Triple Zero delivery, is limited by the TCPSS Act as its principal legislation to only applying to carriers, CSPs and the ECP, and not to mobile device manufacturers (or indeed any other entities or stakeholders).⁹

The obligation to identify and address that failure falls on CSPs under Part 4 of the ECS Determination, not on the manufacturer responsible for the device's configuration. This creates downstream consequences for consumers, who may have their device blocked despite having purchased devices that were compliant at the point of sale.

While CSPs/carriers have responsibility over the underlying network, the only entity with any responsibility over the device specifications (which is a key component in the required ECS Determination configuration assessment) are device manufacturers. Yet the obligation to *identify* any device configuration issues falls entirely on CSPs and carriers.

The result is a scenario where device manufacturers control device firmware and behaviour (including over time via software/firmware updates) despite having no emergency-call related obligations under current legislation, but mobile network operators bear the regulatory and operational burden of, and are accountable for, device issue identification, customer communication, blocking and related customer impacts and management.

The gap between device standards and ongoing network obligations and device management creates a structural mismatch whereby entities responsible for network access (CSPs) are held accountable for failures arising from device-level configuration decisions outside their control.

This structural mismatch has several implications on the ability of CSPs/carriers to comply with their obligations under Part 4 of the ECS Determination, some of which are set out in the following section.

MNOs identifying configuration issues

Given the regulatory compliance obligation is borne by the entities with responsibility over network access (and not device behaviour), outside of basic compatibility issues (such as a

⁹ TCPSS Act, section 147(1), reflected at ECS Determination, section 5(1).

legacy 3G device being non-VoLTE compliant), there are limited ways for MNOs to identify if a particular device is or is not configured to access the ECS. This could include:

- MNO or third party led device testing, which given the broad scope of devices currently available in the Australian market is not practical;
- advice received from the device manufacturers about device compatibility and configuration in network scenarios, although those manufacturers have no legal obligation to proactively provide this information to MNOs (and are similarly not required to engage with MNOs on request); or
- analysis of calls placed on the network by a new device, considering whether that device is demonstrating configuration issues with the ECS, which first requires that the device is present and active on the network for a minimum amount of time for such an analysis to be performed. A device attaching to the network alone is not enough to identify if there is a configuration issue.

Outside of device manufacturer engagement, MNOs have no way of identifying if a particular device is or is not configured to be able to access the ECS until that device is already on the MNO's network, and a failure has been reported.

Reliance on good-faith engagement with device manufacturers for remediations

In practice, and especially in the last 12 months, the device configuration issues which have been identified by MNOs have not been as simple as 'compliant' and 'non-compliant'. In particular, there have been a significant number of devices identified across MNO networks which are, in their current state, not configured to be able to access the ECS, but which are capable of being remediated into a compliant state via device manufacturer software/firmware updates. This has led to outcomes where particular models of mobile phones can be compliant on one software version, but non-compliant on another software version.

The growing classification of devices as 'remediable' in this way is reflective of the non-static nature of device compliance, and highlights that emergency calling performance is increasingly governed by firmware and software behaviour controlled by manufacturers. As above, there are no strict legal or regulatory obligations on device manufacturers to engage with MNOs or remediate mobile phones that have identified device configuration issues (and such a process is entirely outside of the control of MNOs).

Remediable mobile phones are not currently contemplated by the ECS Determination (or other instruments within the Triple Zero framework), meaning there is no scope for the existence (or potential existence) of a remediation update to impact on CSP/carrier obligations to communicate to customers and block non-configured devices under Part 4 of the ECS Determination. Taken together with manufacturers (who are in control of these remediation updates) not being at all governed by the ECS Determination, and the very

short ECS Determination timeframes between issue identification and communications about blocking,¹⁰ there is significant scope for end-users to be exposed to unnecessary service disruptions or inconsistent messaging.

No manufacturer accountability for ECS configuration issues

Given device manufacturers are only currently required to certify their compliance with applicable Australian device standards at a static point in time when first supplied to the Australian market (for the purposes of TLN RCM / SDoC processes), there is no current recognition in the Triple Zero framework nor related technical standards of the dynamic nature of device behaviour and configurations as evolving with continuous software/firmware updates.

Similarly, at the time that mobile device configuration issues are identified (as above, usually after they have been present on an MNO's network already), the device has already complied with applicable TLN labelling requirements and the device manufacturer has no direct legal or regulatory accountability for that device being no longer configured to access the ECS; instead CSPs/carriers bear responsibility for ECS Determination compliance (including customer engagement and management). While manufacturers of more recent devices do have some natural/market incentives to ensure their devices are not blocked on MNO networks (and to therefore work with MNOs in managing configuration issues), this is not equivalent to a legal/regulatory obligations.

Grey imports and unverified devices

A further gap relates to devices purchased from international retailers, whether online, (e.g. online marketplaces), or brought into Australia from overseas by consumers or via unofficial channels (commonly referred to as 'grey' or 'parallel' imports). These devices may not carry the RCM and have not been tested against Australian technical standards. While such devices may appear to function normally across a mobile network using voice/SMS/data, there is no assurance they will be able to contact Triple Zero across that network, or camp on to an alternative network as required.

Australian consumers are generally unaware of this risk, and the current framework provides no mechanism to address it at import or if a configuration issue is discovered. As above, it falls to CSPs/carriers to bear the responsibility of determining whether these grey devices are configured to be able to access Triple Zero in the required conditions. This is practically impossible and unreasonable for CSPs/MNOs to identify and determine the capabilities of all these devices from other markets and countries.

¹⁰ For instance, section 69(2) of the ECS Determination requires a CSP to issue the first notification to end-users of a mobile phone notifying them that the device is no longer configured to be able to access the ECS within 5 business days of the CSP identifying the configuration issue.

What additional requirements should apply

The review presents an opportunity to address these gaps in a structured way. Optus considers the following requirements should be considered:

- The technical standards applicable to mobile devices in AS/CA S042.1 (and related technical standards) should be reviewed more generally by appropriate industry and technical experts to ensure they contain appropriate device standards for emergency calling both in Australia and globally (with a preference to a standardised global approach where practicable).
- Device compliance should be recognised in the technical standards (and associated labelling and compliance requirements) as dynamic and not static at the time of supply to market. In order to maintain their SDoCs (or similar), manufacturers should be required to recertify or attest ongoing compliance with standards following release of major software/firmware updates.
- The process to meet initial and ongoing compliance needs to be reviewed, with appropriate lab-based and Australian live network-based test results taken as part of the compliance assessment validation prior to granting compliance marks.
- Direct obligations on manufacturers under the ECS Determination (or alternative regulatory instruments), extending the framework beyond carriers and CSPs to require manufacturers to take reasonable steps to maintain emergency calling functionality in their devices on Australian networks. In particular, imposing obligations on device manufacturers to provide information and assistance to MNOs where device configuration issues are identified, and in respect of blocking and remediation. This would align regulatory accountability with where device configuration and behaviour decisions are actually made.
- Mandatory notification obligations requiring manufacturers to notify the ACMA and relevant MNOs where a software update, firmware change, or configuration decision may affect emergency calling capability or camp-on functionality on Australian networks.
- An independent device register, as flagged in the consultation paper, that provides a publicly accessible repository of device compliance information, including whether a device has been tested against AS/CA S042.1, its camp-on capability, and its RCM status. This would support MNOs in meeting their Part 4 blocking obligations and give consumers meaningful information before purchasing a device and would also assist in closing the 'grey imports' gap in respect of devices bought online/overseas and which have never been validated against Australian networks or standards.

- Complementary consumer education about the risks of purchasing devices that have not been verified against Australian technical standards, particularly grey import devices sold through overseas / online marketplaces.

The establishment of a device register would address multiple regulatory gaps simultaneously — supporting MNO compliance with Part 4 blocking obligations, improving consumer awareness, and providing regulators with a consolidated source of device capability data to inform decisions about new access methods and future network changes.

Consideration should also be given to strengthening pre-market certification processes to include explicit verification of emergency calling capability across Australian network conditions.

Other devices

Further sitting outside Part 4 of the ECS Determination are other non-handset access modes, such as wearables (e.g. smartwatches). The technical standards that apply to non-handset devices, obligations for identifying configuration issues and undertaking remediation action are some of the issues that should be carefully considered prior to any of these devices being brought into the Triple Zero ecosystem.

INDUSTRY OBLIGATIONS

The current regulatory framework places outcomes-based obligations on carriers, CSPs and the ECP to deliver Triple Zero calls and has begun to move in a more proactive direction. The recent amendments to the ECS Determination that came into force on 1 November 2025 represent a meaningful shift. Optus considers there is a case for further targeted reform to strengthen accountability and proactive risk identification across the ecosystem.

However, any expansion of obligations must be carefully designed. The risk of imposing obligations that are disproportionate, duplicative of existing requirements, or that hold one party accountable for outcomes they do not control is real and would undermine rather than strengthen the framework. Optus supports targeted regulatory refinements that are proportionate and grounded in a clear understanding of who controls what in the Triple Zero call path.

6. 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?

Layered accountability across the supply chain

Further to the principles that should underpin the legislative framework, outcomes and requirements should be proportionate across the entire supply chain. The call path of an emergency call under normal network conditions currently traverses the following:

Device → CSP/Carrier Network → ECP Carrier Network → ECP (Telstra) → ESO

Each step is a potential point of failure. Current accountability is concentrated with carrier networks and at the ECP end. The framework should address this by establishing layered accountability, with each party accountable for the segment they control rather than placing a single end-to-end performance obligation that falls ambiguously across all parties. The following table notes the party with their current accountability.

Party	Current accountability
Device manufacturer / importer	Device capability at point of sale
MNO / Carrier	Access and core network delivery of the call to the ECP handoff point; camp-on availability (mobile network only); network change management
CSP (non-network)	Customer relationship obligations; ensuring access to emergency calling is not impaired by service configuration
ECP (Telstra)	Call answering speed, transfer accuracy, location data handling, ECP-to-ESO handoff

Minimum requirements could be set at each layer, but those requirements should be proportionate to what that party actually controls and the risk at that layer. MNOs should not be held accountable for ECP performance, and vice versa. Similarly, careful consideration

would need to be given to appropriate outcomes or requirements in scenarios where MNOs do not control a key element of call delivery, as would be the case if D2D calls were to be subject to emergency calling obligations.

Caution on end-to-end obligations and over-prescription

Optus urges caution about end-to-end outcome obligations that MNOs cannot fully control. Where a device is untested, purchased from an international retailer without an RCM, or the ECP fails to answer, an MNO cannot guarantee the call reaches an ESO. Any outcome obligation must be scoped to the relevant party's controlled segment of the call path.

Optus also urges caution about over-prescription of how outcomes are achieved. Different MNOs have different network architectures. Outcomes-based standards, such as call completion rate thresholds, are preferable to prescriptive technical requirements that may be appropriate for one network topology but burdensome or operationally irrelevant for another.

Public confidence, education and communications are critical to the ecosystem

Triple Zero is ultimately relied upon by the Australian public during moments of crisis. As the emergency calling ecosystem evolves to include new technologies, access methods and service models, ongoing public education and engagement will become increasingly important. Australians need to understand not only how to access emergency services, but also the capabilities, limitations and appropriate use of different technologies and access pathways. Public confidence in Triple Zero depends on both the reliability of the service and a clear understanding of how it works. The review should consider the respective roles of the Triple Zero Custodian, Emergency Call Person (ECP), government agencies, emergency services organisations and industry in delivering coordinated, ongoing public education and awareness programs.

Optus also considers there is an opportunity to provide greater clarity regarding responsibility for public communications and stakeholder engagement during disruptions affecting the emergency call service. While the framework increasingly defines operational responsibilities across the ecosystem, there is less clarity regarding accountability for communicating with the public, media, governments, regulators and other stakeholders during Triple Zero incidents. As communications play an important role in maintaining public confidence and supporting informed decision-making during critical events, the review should consider the respective roles of the Triple Zero Custodian, the ECP, carriers and government agencies in leading and coordinating external communications. Clear governance arrangements, escalation pathways and communications protocols would support consistent, timely and accurate information sharing while reducing the risk of conflicting messages during incidents.

Optus also recommends that accountability within the Triple Zero framework extend beyond operational delivery and technical performance to include public education, consumer awareness, and communications during incidents, with clear responsibilities assigned to the parties best placed to fulfil those functions.

7. 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?

Principles for any new proactive mechanisms

The recent amendments to the ECS Determination (November 2025) represent a meaningful shift toward proactive regulation. Optus supports a proportionate and structured approach to any further proactive mechanisms; however care should be taken to ensure:

- Any new mechanism demonstrates a clear nexus to Triple Zero safety outcomes, not just regulatory visibility,
- Unnecessary duplication is avoided. Several proactive requirements already exist (Division 5.3 management plans, wilting, outage notifications), and the review should assess whether existing mechanisms are being used effectively before adding new obligations, and
- The risk of duplicative engagement with both ACMA and the Triple Zero Custodian is minimised through a clear delineation of roles and a single point of engagement for carriers where possible.

In general, Optus considers measures targeted at addressing some of the gaps in the regulatory framework identified across the call delivery path are more likely to assist in proactive identification and rectification of issues than post-incident measures.

Incident learnings

In general, incident learnings may be useful where there are particularly unusual or complex incidents, as these are grounded in real-world experience. Consideration could be given to:

- Sharing key learnings across industry, not just to the ACMA, as siloed reporting misses the systemic dimension;
- Calibrating the reporting threshold appropriately, targeting incidents that are more complex or unusual rather than common minor faults; and
- Preserving confidentiality protections for commercially sensitive or national security-related technical information.

Post-outage reporting, outcomes plans and audits

Post-outage reports are unlikely to offer significant insights or learnings where an outage is caused by a natural disaster.¹¹ The current obligation in section 79 of the ECS Determination requiring a post-incident report including an outcomes plan does not make this distinction. While there may be benefits to outcomes plans where outages are caused by issues within the carrier's controlled networks and facilities, the same obligation is of limited utility where the cause was (solely or predominantly) a natural disaster outside the carrier's control.

In many cases post-outage reports may contain the same information provided in outage notifications sent during an outage. It would only be where the cause of an outage is not immediately known or that it may be more complex and more detail may be needed post-outage. Consideration should be given as to whether this remains a requirement for all major outages or if there are only specific circumstances (such as when an outage is not caused by a natural disaster and the cause of the outage is not clearly known) where a more detailed report may be useful.

Optus notes the ACMA already has powers enabling it to conduct audits of compliance with obligations.

Directions

Recent amendments to the ECS Determination give the Triple Zero Custodian the ability to request the ACMA to issue an ECS Direction under section 151A of the TCPSS Act. Given the operational complexities of telecommunications networks and facilities, such directions are likely to be most effective when used as a targeted, last-resort tool rather than a routine regulatory mechanism. Their utility depends in part on being used sparingly and purposefully, and in a targeted manner.

Directions were recently issued by the ACMA on behalf of the Triple Zero Custodian to the three MNOs to provide data related to welfare checks, access to and handling and transfer of emergency calls and welfare checks. This has involved engagement with both the Custodian and the ACMA as the Custodian does not have the power to issue directions itself.

Whether a direction is the best use of obtaining information depends on whether the request is a one-off request (for example, in response to a specific incident or emerging concern) or if data will be required on an ongoing basis. Ongoing data reporting may be best addressed by a record keeping and reporting rule.

¹¹ This is recognised to an extent in the structuring of the *Telecommunications (Customer Communications for Outages) Industry Standard 2024*, which imposes different notification obligations depending on whether the sole or predominant cause of an outage is a natural disaster (see for example section 9(2), and sections 12, 12A and 12B).

REPORTING

Optus supports reporting if it provides meaningful information across the whole emergency call ecosystem. Current arrangements require reporting from MNOs and the ECP provides information under its contractual arrangements and to the ACMA under the ECS Determination which is not publicly available. Reporting obligations should only be imposed where there is a clear benefit outweighing the burden of such obligations. Any public reporting framework should also consider whether disclosure would involve confidential commercial or security information and if transparency can be provided in a general or aggregate way.

8. 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?

Optus suggests any reporting obligations should be focused on the outcomes each party in the call path is responsible for, without being unnecessarily burdensome or revealing commercially or security sensitive detail.

MNOs already provide key reporting

The April 2026 ECS Directions to the three MNOs requires reporting on access to emergency calls, emergency call handling and transfer, and welfare checks. There have been learnings from this process and engagement has commenced on information to be provided under the next direction.

If this information is required on an ongoing basis, it may be worthwhile considering whether a record keeping and reporting rule should be made.

Extending reporting across the ecosystem

Public reporting obligations could also be introduced for the ECP to provide a more holistic picture of Triple Zero performance. The ECP currently reports under a contractual framework that is not publicly transparent. The ECP is subject to detailed performance obligations reported to the ACMA under the ECS Determination and to the Department through its contractual arrangements.

Aligning ECP reporting obligations with those of carriers and CSPs — within the same regulatory framework rather than through a confidential commercial contract — would improve transparency and accountability across the ecosystem, particularly given the ECP's costs are funded through industry levies and per-call charges ultimately borne by carriers and end-users. Transparency of the ECP's performance and costs is a matter of legitimate regulatory interest, not merely a commercial question.

Confidentiality and publication

Any reporting should not be so granular that it reveals commercially sensitive or security-sensitive network information. Transparency should be balanced with appropriate confidentiality protections; for example, aggregated system-level data could be made publicly available without carrier-level attribution, at least in an initial reporting period. Such matters would require further policy consideration.

9. 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?

Device capability information

Information sharing processes should be considered not just for network performance data but also for information about device capability, as device configuration is a critical element of emergency call delivery. As set out in detail in Question 5, regulations currently only require MNOs to take action to identify if devices have configuration issues accessing the ECS and to block those devices, however there is no central registry of such information that encourages consistent action across industry or improves consumer knowledge.

Optus would support establishing an independent device registry to assist consumers in purchasing decisions and MNOs in identifying which types of devices may not be correctly configured to access the ECS. Such a registry could include:

- Device Type Allocation Code (TAC) to capability mapping, providing information on which devices support VoLTE emergency calling and camp-on functionality across which frequency bands
- Supplier SDoC data and endorsed test reports. This information is currently held privately by suppliers and is not accessible by MNOs or consumers
- Data on devices identified as non-compliant by one MNO, which could be shared with other MNOs to allow proactive identification of affected customers across the industry where the device configuration issue is common among mobile networks.

The ATA's DETEST working group is already doing significant work in this area. Further information sharing arrangements regarding devices could build on this work and be formalised and administered by an independent body to ensure credibility over device information and address any competition law concerns around inter-carrier data sharing.

Network outage information sharing

The November 2025 amendments to the ECS Determination introduced requirements for carriers and CSPs to provide information during outages affecting networks that carry Triple Zero calls. Further improvements to how this information is shared could be considered and

we understand the ACMA will be conducting a post-implementation review of these obligations.

One practical improvement would be for the Triple Zero Custodian to manage a central platform through which network operators could supply outage information via API rather than email or other ad hoc channels (as currently required¹²). This information could then be accessed in one place by ESOs and the ECP (and other relevant stakeholders listed in the regulations), providing a more consistent and timely view of network status across all carriers during an active incident (such as a natural disaster). This would reduce burden on individual carriers (allowing them to focus on addressing the outage), improve the quality and timeliness of information available to ESOs for operational decision-making, and give the Triple Zero Custodian better visibility over the state of the ecosystem during a major event.

Governance principles for information sharing

Any information sharing framework must consider existing obligations and, depending on the nature of the information to be shared, applicable confidentiality, privacy and national security considerations. In particular:

- Customer-related data (for example, information about which customers hold non-compliant devices, or that may be related to emergency call connection or camp on calls) must be handled in accordance with the Privacy Act 1988 and the Telecommunications Act 1997 – while it is unlikely this would be needed to be shared, the obligations that apply to carriers/CSPs in respect of this data should be borne in mind.
- Inter-MNO sharing of device capability or network performance data must be structured carefully to avoid competition law exposure (under Part IV of the Competition and Consumer Act 2010), and Optus would support any formal sharing arrangement operating under a safe harbour or with ACCC oversight;
- Information with national security implications, for example, detailed network architecture or failure mode data, should be managed in accordance with existing critical infrastructure obligations and should be held by ACMA with strictly controlled access

Delineating ACMA and Custodian roles

Further clarity between the ACMA's and the Triple Zero Custodian's respective roles in the information sharing ecosystem would be welcome. As both entities have roles in the ecosystem, there is a risk of duplicative engagement and potential confusion for carriers and CSPs. For example, the Triple Zero Custodian has outlined its expectations of providers,

¹² By the Telecommunications (Emergency Call Service) Determination.

however, it is unclear how these expectations align with regulatory obligations and their enforcement.

A Memorandum of Understanding between the ACMA and the Triple Zero Custodian could provide some clarity and define key aspects related to the roles and functions of each organisation, for example:

- How information is shared between the two entities
- Which entity is the primary contact point for carriers during an active incident
- How the two entities coordinate before issuing directions or information requests to carriers

THE LEGISLATIVE FRAMEWORK IMPACT ON ESOs

Changes to how Triple Zero is accessed or how information is shared during outages have direct operational consequences for ESOs, whose systems, capabilities and resourcing are determined by individual state and territory governments.

Optus acknowledges that questions about what works best for ESOs are best answered by ESOs themselves. The following reflects Optus's perspective as a carrier and mobile network operator operating within the Triple Zero ecosystem, focused on the practical implications of the national framework and where improvements may assist both ESOs and carriers in delivering a consistent, reliable service.

10. 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?

Innovation within the national framework

Optus's view is that the national framework does not in itself hinder innovation for ESOs, provided that innovation sits as a layer on top of the existing call delivery path rather than requiring changes to the underlying pathway. The NSW Police Force BluLink service is a good example of this working well; the BluLink service operates as a post-connection layer that allows police to initiate video, text-based messaging and location sharing with the caller once an emergency call is connected to the ESO, without requiring any changes to how MNOs or CSPs deliver the underlying call. This kind of foundation-plus innovation is compatible with a national framework and should continue to be encouraged.

Concerns may arise with new access modes

Key concerns would arise if changes are being considered to the access modes for contacting Triple Zero in the first place. Unlike post-connection enhancements, such as BluLink, changes to access modes require investment and capability upgrades across every ESO in every state and territory before they can be implemented consistently at a national level. This creates a structural challenge: Commonwealth regulation sets the baseline, but the practical ability to deliver against any new access mode depends on state and territory governments investing in ESO systems and capability.

This tension is currently being experienced in relation to Advanced Mobile Location (AML) data, where MNOs transmit precise GPS location information when a Triple Zero call is made, but not all ESOs have the systems capability to receive and use that data effectively. AML is already being transmitted by MNOs, yet the benefit to callers is uneven across jurisdictions because ESO readiness has not kept pace. This is a concrete example of why ESO readiness should be assessed and confirmed as a prerequisite before any new access mode or information type is brought into the regulatory framework (consistent with Optus submissions in response to Question 3).

Addressing such issues in a national system requires significant engagement between the federal government and state and territory ESOs, and sufficient lead time for states and territories to fund and implement the necessary upgrades. This coordination challenge should be explicitly acknowledged in the framework and factored into any decision to expand Triple Zero access modes or information obligations. The readiness of ESOs is a critical pre-requisite before adding any new triple zero access modes or technologies.

11. 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?

Current information sharing obligations

The ECS Determination already includes obligations for information sharing with ESOs. Carriers and CSPs must provide as much information as possible as soon as practicable if an ESO requests information about a call after it has been transferred and must provide the most precise location information available as soon as practicable if an ESO requests location data for an emergency call. The November 2025 amendments to the ECS Determination further introduced outage information sharing requirements.

Optus does not consider there is a significant gap in the categories of information that carriers are required to share with ESOs under the current framework. The more pressing issue in practice is the timeliness, format and consistency of information sharing, particularly during active outage events, which is addressed in Optus's response to Question 9.

Welfare checks

Optus would welcome further clarity around the welfare check framework. The current obligations — section 28 of the ECS Determination requiring CSPs to undertake a welfare check where a major outage is identified, and section 55 requiring the ECP to undertake a welfare check where there is a disruption to the ECS and a caller has connected to the ECP's system — provide a minimum baseline. However, feedback from the Custodian's engagement with MNOs and ESOs has highlighted inconsistency in welfare check expectations and processes across industry, and that MNO decisions to go beyond minimum obligations can create additional and unpredictable burdens for ESOs.

Optus supports a consistent, principles-based welfare check framework that:

- Clearly defines the triggers for a welfare check, distinguishing expectations between different outage types and severity levels
- Ensures standard information is provided to ESOs when a welfare check is referred, so ESOs can action referrals efficiently and consistently
- Clarifies the division of responsibilities between MNOs, the ECP and ESOs at each stage of the welfare check process

Public

- Addresses what obligations, if any, apply outside of major outages, including where individual carriers or CSPs choose to go beyond regulatory minimum requirements

Optus welcomes further engagement with ESOs on this aspect to ensure there is a nationally consistent and operationally manageable approach to welfare checks. Given that welfare check obligations impact ESOs directly, any reform in this area should be developed in close consultation with ESOs before regulatory changes are made.

REGULATORY OVERSIGHT OF TRIPLE ZERO

Optus supports an effective and predictable regulatory framework for Triple Zero. The question may not be what additional powers are required, but, whether the ACMA or Triple Zero Custodian are currently constrained from acting in a way that has demonstrably resulted in, or would have prevented a specific failure.

The Optus Outage Review (Bean Review)¹³ identified several improvements across the Triple Zero regulatory framework and the changes resulting from it have only been in place for a short time. The ACMA already holds broad and flexible powers; the Triple Zero Custodian has only been operational since October 2025; and the suite of regulatory changes introduced in late 2024 and 2025 have not yet been subject to a post-implementation review.

Any expansion of powers should be the result of a clearly identified need that cannot be addressed by existing powers. Poorly designed powers risk creating regulatory uncertainty, duplicative compliance obligations, adding to cost burden, and potentially chilling network investment and technological adoption if there is an unpredictable enforcement environment.

12. 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?

ACMA's existing powers are broad

The ACMA already holds broad powers in relation to:

- Part 27 of the Telecommunications Act 1997 (information gathering);
- Section 12 of the ACMA Act (an open-ended power to do 'all things necessary or convenient' in connection with the ACMA's functions);
- ECS Direction power (section 151A, TCPSS Act) (compulsion powers in relation to Triple Zero matters);
- The ECS Determination under section 147 of the TCPSS Act (including the ability to amend the determination within its established principles and with prior consultation);
- Enforcement powers under the Telecommunications Act and TCPSS Act; and
- Industry Code enforcement powers.

¹³ Mr Richard Bean, Review into the Optus outage of 8 November 2023 – Final Report, March 2024.

Available at:

https://www.infrastructure.gov.au/sites/default/files/documents/review_into_the_optus_outage_of_8_november.pdf

On the basis of these existing powers, Optus does not consider that ACMA requires significant additional regulatory powers at this stage. The more productive focus for this review is on ensuring that the ACMA has the inter-agency coordination arrangements needed to use its existing powers proactively, as addressed in Optus's responses to Questions 7 to 9.

One identified gap

That said, as previously noted in response to Questions 5 and 6, there is a gap in ACMA's ability to directly regulate device manufacturers under the ECS Determination. The TCPSS Act does not currently enable ACMA to impose obligations on device manufacturers in relation to Triple Zero, meaning that where devices are not configured to access the ECS, ACMA cannot require the manufacturer to take corrective action or share information about the configuration issue. This gap is increasingly problematic given that device configuration decisions are a critical and growing source of risk in emergency call delivery.

Addressing this specific gap by extending ACMA's powers under the TCPSS Act to cover device manufacturers in relation to Triple Zero obligations would be a targeted and justified expansion. It would not require a wholesale expansion of ACMA's enforcement remit but would close a specific legislative gap that the current framework cannot adequately address.

13. 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?

Optus is not aware of specific legislative barriers preventing the ACMA from taking a systemic view of Triple Zero issues or from linking related infringements. The ACMA's existing powers appear broad enough to consider patterns of behaviour across multiple incidents and to treat related breaches as indicative of a broader systemic problem.

Practical rather than legislative barriers

In practice, any barriers are more likely to be administrative rather than legislative. The introduction of a Memorandum of Understanding between the ACMA and the Triple Zero Custodian (as recommended in response to Question 9) would ensure that systemic issues identified by either entity through their respective oversight and monitoring functions are shared with the other, rather than remaining siloed.

If the post-implementation review of the 2024–2025 regulatory changes identify specific procedural barriers to the ACMA taking a systemic enforcement approach, these should be addressed in a targeted way rather than through legislative change, for example, through enforcement guidelines or an industry guidance note.

14. 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?

Too early to conclude the balance is wrong

The Triple Zero Custodian was established in October 2025, with changes to the ECS Determination resulting from the Bean Review occurring in late 2024 and late 2025. Optus understands that a post-implementation review of these changes is expected.

To date, there have been two ECS Directions issued by the ACMA on behalf of the Custodian – we understand the ECS Direction issued in April 2026 required the same data from each MNO. It is still relatively early to conclude that the balance between the ACMA and the Custodian is wrong or that legislative change is needed. The framework deserves the opportunity to bed down before further structural changes are made.

Issues that may result from an ecosystem that includes the ACMA and Triple Zero Custodian are the risks of duplication if there is a lack of coordination, overlapping functions, or inconsistent guidance to industry. The roles and functions of each organisation should seek to maintain the conceptual distinction between the two with the ACMA as regulator/enforcer, and the Triple Zero Custodian in its general oversight and coordination roles. We would welcome clarifying the administrative arrangements between the two organisations, for example, by way of a Memorandum of Understanding.

Revisiting the original policy intent

That said, given the significant thought that was put into the role and functions of the Triple Zero Custodian during its development, the original policy intent behind the ACMA/Custodian architecture should be revisited to assess whether that intent is being realised in practice. That is, the Custodian having a coordination role, particularly during an outage, and the ACMA remaining as the enforcement organisation.

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

The Triple Zero Custodian's powers under the TCPSS Act (see Division 5 of Part 8) include:

- Requesting the ACMA to issue ECS Directions
- Compelling the provision of information from ACMA in support of its functions
- Overseeing the effective functioning of the ECS and related matters
- Advocating for best practice processes, policies and procedures
- Aiding preparation for, response to, and recovery from outages affecting the ECS

These powers would appear to be sufficient to fulfil the Custodian's role. The Custodian has been operational for less than a year and Optus is not aware of any instance in which the Custodian's existing powers have proved insufficient to perform a function it has sought to undertake. Any expansion of the Custodian's powers should be based on evidence of a specific function the Custodian has been unable to perform using existing measures, or that the ACMA has been unable to perform through its own powers and the existing referral mechanism under section 151L of the TCPSS Act.

There should also be demonstrated evidence that any proposed new powers would not duplicate or overlap with the ACMA's existing powers. Duplication increases the risk of regulatory uncertainty, compliance inefficiency and unnecessary organisational overlap between the two entities; outcomes that would be contrary to the intent of the ACMA/Custodian architecture.