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

TRIPLE ZERO CUSTODIAN

SUPPLEMENTARY SUBMISSION TO THE ENVIRONMENT AND COMMUNICATIONS REFERENCES COMMITTEE

February 2026

Background

The Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department) previously provided a submission to the Senate Environment and Communications References Committee's inquiry into Triple Zero service outages on 24 November 2025. Departmental officials subsequently appeared before the Committee at a public hearing on 9 December 2025. The department welcomes the opportunity to provide this supplementary submission to assist the Committee in its further consideration of matters raised during that hearing.

This supplementary submission responds to questions and themes raised by Senators during the hearing by providing additional clarification on the respective roles and responsibilities of participants across the Triple Zero ecosystem. It does not seek to restate matters in the original submission or pre-empt the findings of ongoing investigations.

Custodian responsibilities in crisis response and outage management

In a crisis, the Triple Zero Custodian (the Custodian) ensures relevant information flows rapidly across the sector, appropriate escalation pathways are followed, and government stakeholders are kept informed of any risks to the continuity of Triple Zero access.

Outage notifications are managed through a structured model that provides continuous logging and escalating of issues reported by carriers. Notifications are recorded in an Outage Notification Log, with escalation decisions made according to the scale and nature of the incident.

The Custodian has provided Mobile Network Operators (MNOs) with notification protocols to ensure clear expectations regarding communications to departmental stakeholders for events affecting the Triple Zero system, as opposed to broader network outages.

Throughout an event, the Custodian ensures concise, accurate information is shared with carriers, Ministerial staff and emergency service partners, and prepares situation reports for all disruptions and major outages. This approach supports effective coordination and clear accountability during Triple Zero disruption incidents.

The Australian Communications and Media Authority's (ACMA) role is to identify, investigate, and take enforcement action for non-compliance by telcos with their obligations under the law, including those focussed on access to the emergency call service.

Welfare check responsibilities in the emergency calling ecosystem

The emergency calling system in Australia involves numerous actors, including telecommunications carriers, emergency service organisations, including state and territory police, and the Commonwealth. Telecommunications carriers are legally responsible for the operations and resilience of their networks to ensure that emergency calls can be carried at all times. Carriers are also responsible for detecting network faults that may affect access to Triple Zero.

Under the Telecommunications (Emergency Call Service) Determination 2019 (ECS Determination), carriers also have specific obligations relating to welfare checks following a major outage where emergency call attempts are unsuccessful. Carriers also implement internal business policies which lead to each undertaking welfare checks over and above the regulatory requirements in the Determination. Carrier welfare checks are undertaken remotely and involve attempts to contact the caller using the contact details available within the carrier's system, to confirm whether assistance is still required.

Where a carrier is unable to establish contact or confirm a caller's welfare, it must be escalated to emergency service organisations, including state and territory police, for further action. Police may then undertake physical welfare checks, consistent with their jurisdictional responsibilities.

Privacy considerations following a Triple Zero disruption incident

Information sharing after an emergency calling incident is governed by strict privacy frameworks across the telecommunications, health and law-enforcement sectors, which also dictate if, when and how personal information can be disclosed. Consequently, the department typically receives only de-identified data for telecommunications oversight purposes, rather than caller-specific health outcome information. Specific information pertaining to an incident ultimately and appropriately remains in the purview of the relevant State Government authorities.

Distinguishing Triple Zero call failures from network coverage limitations

The Triple Zero service received 14.6 million calls in 2025, of which 11.7 million calls were answered by the Emergency Call Person (ECP) (the difference being misdials, caller terminated calls etc.). Of these 11.7 million calls answered, just over 9 million were transferred to State and Territory Emergency Service Organisations. The majority of calls to Triple Zero are made from mobile phones rather than, as they were in the past, from landlines.

Triple Zero call failures occur when an emergency call is initiated on a network, but not successfully carried through to the ECP. These failures can arise for a range of reasons, including network outages (affecting all calls, not just Triple Zero calls), network congestion, lack of coverage, or network and device configuration.

Network coverage issues occur when there is insufficient or no signal from any carrier which prevents calls from being initiated, whether emergency or routine. Coverage gaps are primarily a function of infrastructure availability, geography and investment decisions.

Network coverage expansion and signal availability are addressed through broader telecommunications policy and infrastructure programs within the department, rather than through the Triple Zero Custodian function. The Custodian's role focuses on how emergency calls are handled once a service is available, including testing, recovery arrangements and camp-on functionality. Where gaps are identified in the delivery of emergency calls the Custodian will act to redress these gaps.

The 3G network closure and device impacts

The decision to shut down the 3G networks in 2024 was a commercial decision by Telstra, Optus and TPG Telecom to repurpose 3G spectrum to expand their 4G and 5G networks.

Prior to the shutdown, the Government worked closely with industry and required assurances from all carriers that 4G coverage would meet or exceed existing 3G coverage in their published coverage maps, emergency calls would remain reliable, and customers with affected devices would receive adequate advance notice and support.

Prior to the shutdown, MNOs identified a number of phones that relied on 3G networks for emergency calling functionality. These phones would have been unable to call Triple Zero in any circumstances following the closure of the 3G networks.

To protect public safety and to ensure all phones connected to mobile networks could call Triple Zero, the former Minister for Communications directed the ACMA to amend the ECS Determination to require service providers to identify mobile phones that are unable to access Triple Zero, notify the user and cease providing a service to the affected device. The amendment came into effect in October 2024. This is the first time that carriers have been required to identify devices on their networks that would be unable to call Triple Zero.

The department understands that around 276,000 devices were blocked immediately after 28 October 2024, when 3G was fully switched off. The MNOs will be able to provide more accurate figures on the volume of devices blocked from their respective networks. Affected devices were a subset of the more than 30 million mobile phones in operation in Australia.

Communication by carriers directly to their customers about the need to block these devices was considered to the most effective way to clearly communicate the changes, and to avoid the risk of the ECP being overwhelmed by test calls.

Samsung device software configuration issue

On 20 October 2025, Telstra advised the department and ACMA of a software configuration issue affecting a limited set of older Samsung handset models.

Telstra's testing showed these devices may not correctly connect to Triple Zero in the very unlikely event both the Telstra and Optus networks are unavailable, but that Vodafone coverage is available, and the device must connect via Vodafone's network to make a Triple Zero call (utilising camp-on functionality). Telstra advised some affected Samsung models can be remediated via software updates, while others cannot.

It should be noted that this is a separate issue to the concerns which led to the amendments to the ESC Determination in advance of the 3G network closures: as noted above, the devices in those cases would have been unable to call Triple Zero in any circumstances.

The MNOs are managing the resolution of this issue. Devices that can be fixed through a software update will remain in service once updated. Users of devices that cannot be remediated will be notified of such and their services ceased consistent with the requirements of the ECS Determination. Users of devices which could be updated, but to which services are ceased as the user has not done the update by the mandated date for carriers to cease supplying a service, can have their services restored at a later date if the user does the required software update over a wi-fi connection.

Carriers have advised the department that there are approximately 49,000 Samsung devices where a software upgrade to overcome the issue was not possible, and would therefore need to be blocked. Carriers are offering affected customers a range of support, such as discounted replacement devices.

Emergency calling limitations for overseas handset variants

Some devices currently in use in Australia are overseas or non-Australian variants of mobile phones brought into the country by consumers, including devices purchased second-hand or originally supplied for use in other markets.

While some of these devices appear identical to Australian-sold models, they can differ in technical characteristics critical to emergency calling in Australia, including network behaviour, firmware and carrier configuration profiles.

Where a carrier cannot verify a device's emergency calling performance due to variant-specific differences or a lack of supported software, service must be withdrawn. As a result, overseas or non-Australian handset variants may continue to be blocked under the ECS Determination, even where a closely related Australian-sold model remains supported.

TPG Telecom/Vodafone Triple Zero call failure incident – 24 September 2025

On 24 September 2025, a TPG customer attempted to call Triple Zero using a Samsung device in Wentworth Falls, New South Wales, but the call did not connect.

Departmental enquiries to TPG and Telstra confirmed no network outage had been detected. The failure was ultimately attributed to the handset's outdated software, which had not been updated.

The department notes and respects the privacy of the persons involved in the incident and does not wish to cause any further distress. As noted above, privacy requirements appropriately restrict the information available to the Custodian, and it does not have full information about the health aspects of the incident. The information provided to the Custodian to date by TPG, Telstra and NSW Ambulance does not enable the Custodian to ascertain whether the Triple Zero calls were made before or after the person died, nor who made the calls.

Every failed call to Triple Zero is a concern to the Custodian, even when not associated with the death of a caller. Failed calls indicate an error in one, or multiple parts of the complex Triple Zero ecosystem and it is the role of the Custodian to ensure each actor in the system undertakes their requirements to identify and address these errors. The Custodian has strong information gathering powers in this regard.

In the case of this incident, the Custodian sought more information from the caller's MNO, and engaged with the ACMA. This included sharing concerns that the incident may indicate a wider handset issue requiring investigation/remediation.

As a result of these queries, the ACMA and MNOs investigated the matter further, leading to identification of the problem and a series of solutions instituted by the MNOs. These investigations led to the identification of the software configuration issue affecting a limited set of older Samsung handset models, as advised by Telstra on 20 October 2025.

This outcome reflects the proper operation of the Custodian. The Custodian is not the regulator but ensures that different parts of the ecosystem are working together to learn from any failures, whether they be large-scale network outages or single failed calls, and to implement solutions.

The ACMA is currently investigating this incident for any failures of regulatory compliance.

Future areas of work and improvement for the Custodian

Public awareness and information

Strengthen public information and education initiatives to improve community understanding of Triple Zero access, including device capability, network behaviour and actions to take during outages.

Legislative and regulatory review (Bean Review Recommendation 18 – In Train)

Progress the review of all legislation and regulation relating to Triple Zero, informed by lessons from the 2023 and 2025 Optus outages, the 3G network shutdown, device specific issues and ongoing testing conducted by UTS.

Mobile network operator and handset operator activities

Support ongoing work by MNOs and handset manufacturers to identify device related issues and implement remediation measures, including through software updates or device replacement where required.

The department will continue its work with UTS to strengthen network and device testing, ensuring that a broader range of devices can reliably connect to Triple Zero and reducing unnecessary device withdrawal or replacement.