Telstra submission

Environment and Communications References Committee inquiry into the:

Triple Zero service outage

Public submission

25 November 2025

Contents

Executive Summary

Telstra welcomes the opportunity to provide this submission to the Senate Environment and Communications References Committee (Committee) inquiry into the Triple Zero service outage (Inquiry). As Australia's Emergency Call Person (ECP) under government contract, Telstra is responsible for providing the national Triple Zero call centre as the first point of contact for the emergency call service (ECS). Our submission focuses on Telstra's role as the ECP, our response to the Optus network disruption on 18 September 2025, and broader issues affecting the resilience and reliability of Australia's ECS.

We recognise the critical importance of reliable telecommunications for all Australians, particularly those in regional and remote communities. The ECP's processes and systems are designed to meet strict legislative and service level requirements, ensuring that emergency calls are answered promptly and efficiently, even during network disruptions. During the 18 September 2025 incident, the ECP's, and Telstra's, systems operated as intended, with no evidence of missed or failed emergency calls at the ECP or within our network. Once we were advised of an issue in Optus' network, the ECP's monitoring and welfare check processes were activated, and we maintained close communication with emergency service organisations (ESOs) and government stakeholders throughout the event.

Our submission also addresses the implementation of recommendations from the Bean Review and recent regulatory changes, highlighting Telstra's compliance with new obligations and ongoing commitment to continuous improvement. We detail the measures taken to enhance the resilience of the Triple Zero ecosystem, including investments in network diversity, real-time monitoring, and operational redundancy.

Furthermore, we discuss the opportunities and limitations presented by roaming, temporary disaster roaming, and emerging technologies such as low earth orbit satellite services. Telstra supports innovation in these areas, while emphasising the need for careful management to avoid unintended consequences, such as network overload during disasters.

Finally, the submission explores the complexities of consumer device compliance and the importance of robust regulatory frameworks to ensure all Australians can reliably access emergency services, regardless of device or location. We recommend that the ACMA collect and publish Declaration of Conformity statements, to provide all Australians and mobile network operators (MNOs) better visibility of the devices that have met the obligations of the Telecommunications Labelling Notice scheme.

Telstra remains committed to working collaboratively with government, industry, and the community to strengthen Australia's emergency telecommunications and ensure the safety and wellbeing of all Australians.

1 Introduction

We welcome the opportunity to provide this submission to the Senate Environment and Communications References Committee (Committee) inquiry into the Triple Zero service outage (Inquiry). Telstra, under government contract, is the ECP and is responsible for the national Triple Zero call centres as the first point of contact for emergency calls. Consequently, our submission focuses on our role as the ECP, and our involvement on 18 September 2025 when Optus experienced a network disruption (the Optus Incident).

The Terms of Reference for the inquiry are broad, encompassing topics as diverse as roaming and the adequacy of regulatory and legislative frameworks. To this end, our submission includes a brief discussion on roaming, temporary disaster roaming, new technologies such as low earth orbit satellite services, and some thoughts regarding making the device compliance regime more transparent and accessible for mobile network operators and Australian consumers.

Our submission is structured as follows:

- Section 2 describes Telstra's role as the ECP and the functions of the ECP;
- Section 3 details what we observed of the Optus Incident and how we reacted;
- Section 4 details our current compliance with legislative requirements, including the *Telecommunications (Emergency Call Services) Determination 2019* (as amended in 2025)[1] (the ECSD) and the *Telecommunications (Customer Communications for Outages) Industry Standard 2024* (as amended in 2025)[2];
- Section 5 details an outage to the ECP on 1 March 2024, where thousands of personal medical alert devices (pendant alarms) overwhelmed the ECP with test calls;
- Section 6 discusses roaming and temporary disaster roaming; and
- Section 7 contains some suggestions on device compliance and a short overview of the Samsung device issue.

2 Triple Zero and Telstra's role as ECP

This section of our submission describes our role as the ECP, and explains the Triple Zero Disruption Protocol, which has been developed by Telstra as the ECP in collaboration with industry to guide immediate actions in the event of a disruption to the ECS.

The Triple Zero ecosystem has three key components. Telstra has a role in each of the components:

- As a carrier and carriage service provider (CSP), Telstra has obligations to maintain its network and facilities that are used to carry emergency calls and to carry emergency calls to the ECP. All carriers and CSPs in Australia have this responsibility on their networks.
- As ECP, Telstra has obligations to receive and answer emergency calls made to Triple Zero and transfer those calls to the appropriate ESO.
- Where Telstra provides connectivity to an ESO (downstream of the ECP), to ensure emergency calls are transferred from the ECP to the ESO.[3]

1 Compilation No 4, Compilation date 1 November 2025. Available at: https://www.legislation.gov.au/F2019L01509/latest/text.

2 Compilation No 1, Compilation date 30 June 2025. Available at: https://www.legislation.gov.au/F2024L01447/latest/text.

3 Note: Other service providers also provide downstream connectivity to some ESOs. We welcome this diversity and consider there is room for additional diversity on the downstream side of the ECP by ESOs maintaining services with multiple service providers.

In this submission, we are focused on the ECP and how it relates to the Optus Incident (in Optus' carrier network) that impacted uphill calls.

2.1 Telstra's role as the ECP

Telstra acts as the ECP under a government contract, and is responsible for providing the ECS, including receiving and handling all emergency calls made to Triple Zero in Australia. Telstra delivers this responsibility through three dedicated Triple Zero call centres located in Sydney, Melbourne and Adelaide.

In FY25, the ECP answered around 11.7 million calls, which is an average of 32,000 per day. This represents a 22% increase in the number of calls answered since FY20.

As the ECP, Telstra must meet strict service levels, ensuring that emergency calls are answered quickly and efficiently—85% within 5 seconds and 95% within 10 seconds. In the most recent reporting period (October 2025), Telstra exceeded these targets, answering 97% of calls within 5 seconds and 98% within 10 seconds on all days other than 31 October 2025. This was due to a significant storm event in Queensland. All performance requirements were exceeded every day for the previous 6 months.

The ECP's primary function is to receive emergency calls from across all networks and promptly connect callers to the appropriate ESO being police, fire, or ambulance. Telstra's processes and procedures are designed to comply with legislative requirements and to ensure the reliability and effectiveness of the ECS. Telstra continually reviews and updates its systems to maintain high standards of service and public safety.

2.1.1 Welfare checks

Calls to Triple Zero occasionally experience a failure, such as a call dropout, and are unsuccessful. Most dropouts are due to circumstances such as a user hanging up after accidentally dialling Triple Zero or where a user has poor or intermittent mobile coverage. Monitoring processes are used to detect these failures to trigger a welfare check process. Telstra conducts welfare checks on an incident-by-incident basis, by following established escalation procedures and communicating with relevant ESOs. This may include attempting to reconnect with the caller, notifying the relevant ESO, and, where the caller cannot be reconnected with, requesting a welfare check to be undertaken by the police to verify the safety of the caller or any persons involved. Each welfare check is documented and reviewed internally, with outcomes used to inform improvements.

2.2 Triple Zero Disruption Protocol

The Triple Zero Disruption Protocol (TZDP or Protocol)[4] has been developed by Telstra as the ECP for the ECS in collaboration with the industry to guide immediate actions in the event of a disruption to the ECS. This protocol complements the disruption protocols requirements under section 81 of the ECSD.

The Protocol sets out a framework for communications and decision making across the Triple Zero ecosystem, with clear roles assigned to the key stakeholder groups. The trigger for the Protocol is the identification of an ECS Disruption, by the ECP, an ESO, and/or a carrier/CSP. An ECS Disruption, for the purposes of the Protocol, is defined as, "*a disruption to the ECP's ability to answer and process emergency calls*".

The Protocol focuses on stakeholder communication and responsibilities and excludes the technical resolution of an ECS Disruption. It covers the key activities and requirements needed to effectively manage stakeholder communications in the event of an ECS Disruption, including industry preparation

[4] Contains sensitive information, not publicly available.

for an ECS Disruption, management of communications throughout the event, and communications required at the conclusion of the ECS Disruption.

The Protocol does not cover the welfare check process for major outages which a CSP is required to conduct pursuant to section 28 of the ECSD.[5] The welfare check process is covered by the Australian Telecommunications Alliance (ATA) Industry Guidance Note *Escalated Welfare Checks* (IGN018:2025),[6] which provides the process and police contacts. Also, the Protocol does not cover communities in isolation, as these events are managed by the relevant CSP.

At its earliest stage, the ECP or ESOs will identify a potential disruption to normal operations of the ECS. In other cases, a carrier/CSP will identify a potential disruption to their network impacting normal operations of the ECS (namely, inability to deliver calls to the ECS) and, in this case, it is expected that the carrier/CSP would advise the ECP directly of the disruption.

The ECP will confirm if the ESO Partner Bridge should be convened. The ESO Partner Bridge is a teleconference facility that brings key stakeholders together via a voice call to share information in relation to an event. This may be done in consultation with the ESOs, depending on circumstances of the event. ESOs or carrier/CSPs may request that the Protocol is invoked by directly contacting the ECP.

A detailed timeline of the Optus Incident as it was communicated to the ECP, is set out in section 3.2 below.

3 Telstra's visibility of the Optus Incident and its response

This section of our submission outlines Telstra's visibility of the Optus Incident and our response. We start with a brief description of the function of our Triple Zero Incident Operations team, followed by a timeline of the Incident.

3.1 Triple Zero Incident Operations

Our Triple Zero Incident Operations team is responsible for managing the network equipment that provides the ECP capability, as well as monitoring the overall performance of Triple Zero calling within Telstra's networks. They are the point of contact for other carriers to manage Triple Zero calling and perform the investigation of unsuccessful Triple Zero calls as part of the welfare check process.

The Triple Zero Incident Operations team receives multiple notifications from network carriers daily, advising them of significant local outages (SLOs). On 18 September 2025, the Triple Zero Incident Operations team received a total of 16 notifications (inclusive of two from Optus), and on 19 September, the Triple Zero Incident Operations team received a total of 25 notifications. These notifications are from all carriers (including Telstra), and are required under the **Telecommunications (Customer Communications for Outages) Industry Standard 2024**,[7] brought into effect in two tranches on 31 December 2024 and 30 June 2025 respectively.

It is worth noting that these amendments have driven a significant increase in the number of notifications daily. Triple Zero Incident Operations currently receive notifications for all major outages and significant local outages from all carriers. To be clear, the increase in volume is not a result of more outages; rather,

---

5 Section 28 provides that a CSP must, as soon as practicable after (a) becoming aware of a major outage that adversely affects a controlled network or facility that the CSP owns or operates or (b) being notified of a major outage under section 8 of the CCO Standard, undertake (or arrange to be undertaken) a welfare check.

6 ATA Industry Guidance Note 018 (IGN018_2025). Escalated Welfare Checks. Available at: https://www.austelco.org.au/ign018_2025-escalated-welfare-checks/.

7 Telecommunications (Customer Communications for Outages) Industry Standard 2024 (as amended in 2025), Compilation No 1, Compilation date 30 June 2025. Available at: https://www.legislation.gov.au/F2024L01447/latest/text.

it is a change in reporting under the Customer Communications for Outages Industry Standard that requires dozens of notifications to be processed daily, to identify which are impactful and which are not.

3.2 Timeline of the Optus Incident

The ECP was first alerted of the Optus Incident via SMS at 14:19:47 AEST, 18 September 2025. There were two messages from Optus:

- 14:19:47 - “Heads up: we've just identified an issue with Triple Zero calls from SA & WA, possibly since 3am today. Networks team investigating. We're commencing welfare checks.”
- 14:19:48 - “Issue now resolved by rolling back a network change. It appears only ~10 TZ calls impacted. We've notified ACMA, SAPOL & WAPOL as well.”

Following these two messages to the ECP, Telstra’s Triple Zero Incident Operations team received a phone call from Optus at 15:17 AEST on 18 September. During the phone conversation, Optus advised they had an issue and had sent us an email. Triple Zero Incident Operations advised no email had been received and confirmed the correct Triple Zero Incident Operations inbox address. During the phone conversation, Optus did not provide any advice about impact, volumes or restoration. At this time, Triple Zero Incident Operations did not ask further questions, as they were waiting for the email for further information.

At 15:26 AEST, Triple Zero Incident Operations received the forwarded email below from Optus. The timestamp on the original email was 15:17 AEST, 18 September 2025. The email stated the incident was resolved at 14:34 AEST, although the date of 19/09/2025 was incorrect, and was subsequently corrected (see below). Note: The email address of Triple Zero Incident Operations is redacted to preserve its confidentiality in this public submission. Additionally, the reason the email was resent as a forwarded mail is that there was a single letter error in the email address entered by the sender in the initial email at 15:17 AEST.

From: [redacted]
Sent: Thursday, 18 September 2025 3:26 PM
To: [redacted];
Subject: RE: Significant Network Outage Affecting 000 Emergency Calls - Open/Resolve notification

\+ [redacted]

From: [redacted]
Sent: Thursday, 18 September 2025 3:17 PM
To: [redacted]
Subject: Significant Network Outage Affecting 000 Emergency Calls - Open/Resolve notification

Optus advises that it has become aware of a Significant Network Outage that adversely affects the carriage of emergency calls over the Optus network before handover to the Emergency Call Person. This notification is in accordance with Section 27 of the Telecommunications (Emergency Call Service) Determination 2019 (“Determination”) This incident has now been resolved.

Incident number IM1919357 commenced at 00:40 AEST and resolve at 14:34 AEST on 19/09/2025

> Mobile users unable to dial Emergency calls from South Australia, Western Australia, and Northern Territory.

Triple Zero Incident Operations forwarded the email to the ECP and the National Operations Manager, Telstra Triple Zero, on 18 September at 15:36 AEST and copied it to Triple Zero Incident Operations stating "*FYI, we haven't seen any issues from our end and no unusual number of welfare checks detected during this time*."

At 15:27 AEST, a second email (below) was received by the Triple Zero Incident Operations team from Optus in relation to the Incident:

> **From:** [redacted]
> **Sent:** Thursday, 18 September 2025 3:27 PM
> **Subject:** RE: Significant Network Outage Affecting 000 Emergency Calls - Open/Resolve notification
>
> Team,
>
> Correction to the date:
>
> **Incident number IM1919357** commenced at 00:40 AEST and resolve at 14:34 AEST on **18/09/2025**
>
> Thanks,

When Triple Zerio Incident Operations receive outage notifications, such as those above, they conduct a series of internal checks. These include monitoring call volumes, identifying any spikes in welfare check activity, and reviewing system performance for anomalies that may provide insight into the reported issue. If we detect an impact within our network or observe unusual welfare check activity, we escalate for guidance and initiate incident management processes as required. Where appropriate, we also provide supporting information or statistics to other carriers.

In the case of the Optus Incident, limited detail was provided. As we later learned, calls were failing before reaching Telstra's network, and hence, before reaching the ECP. At the point where we were notified, overall call volumes were within normal ranges, and prior to the notifications, call volumes had not altered beyond normal daily fluctuations.

3.3 Camp-on, failed calls and volume of emergency calls during the Optus Incident

In FY25, the ECP answered around 11.7 million calls, which is an average of 32,000 per day. Due to the volume of calls impacted[8] by the Optus Incident and the time of day, the variation in call volumes was within the range of normal traffic variations that occur every day.

To illustrate, we reviewed the number of Optus calls received to the ECP between 12:00AM Monday 8 September and 11:59PM Thursday 18 September (i.e., the 10 days prior to, and inclusive of the day of the Optus Incident). In that 10-day window, the highest volume of calls, 8002 occurred on Saturday 13 September. We would expect this, as Saturdays are traditionally the ECP's busiest day of the week. The lowest volume, 6,650 occurred on Thursday 18 September (i.e. the day of the Incident). However, by comparison with the 6,719 calls on the previous Thursday (11 September 2025), there was a difference of only 69 calls (approximately 1%) between consecutive Thursdays. With an average of 32,000 calls received each day, the "missing" calls were not evident statistically.

[8] i.e., the volume of emergency calls from Optus customers that did not reach Telstra's network, and hence, the ECP.

3.3.1 No discernible rise in "camp-on" traffic

Optus' submission notes that 66 of the 605 unique service numbers were able to camp-on to another network.[9] Across all the camp-on and normal calls, a rise of 66 calls across WA, SA and NT over a 14-hour period is not discernible. As such, there were no abnormal patterns to alert us ahead of Optus contacting us.

3.3.2 No failed emergency calls recorded at the ECP

Under s.27 of the ECSD (which was in force at the time of the Optus Incident), impacted carriers and CSPs were required to notify (or arrange to notify) the ECP as soon as possible after becoming aware of a significant network outage[10] occurring within the network they own or operate and use to carry emergency calls or supply emergency telephone services. Telstra does not have visibility of alarms or performance metrics within other carriers' networks.

Within Telstra's network, the ECP welfare check process continuously monitors for emergency calls from Telstra's network and other carriers (monitored at the interconnect gateway, which is the extent of our monitoring visibility) that fail to progress or complete as expected. Alarms are generated for calls that fail. During the fourteen hours of the Optus Incident, there were no calls identified as entering our network (via the interconnect gateway) that did not reach the ECP.

3.3.3 No discernible drop in emergency calls from Optus

The ECP has a performance dashboard which monitors the volume of emergency calls received, but there was no discernible reduction in traffic during the Optus Incident.

3.4 Other engagement

Telstra first became aware of the full extent of the Optus Incident, including that more than 600 calls had failed to reach Triple Zero across three states and that fatalities were involved, through Optus' media conference on the afternoon of Friday 19 September 2025.

As noted above, our technical teams had already verified that all Telstra systems, including the Triple Zero switching and routing infrastructure were fully operational and functioning normally. See the end of section 3.2 for details.

On the evening of Friday, 19 September, Telstra provided confirmation to State and Federal government stakeholders there were no issues with the Triple Zero platform or call camp-on.

Telstra was then in contact with the Government in the days following the Optus Incident to respond to enquires related to our role as the ECP.

4 Implementation of Bean Review recommendations

This section of our submission addresses item d) in the terms of reference for this inquiry.

> d) the implementation of recommendations of the Australian Government Review into the Optus Outage of 8 November 2023 (Bean Review) and the September 2024 inquiry report by the Environment and Communications References Committee into the Optus network outage;

[9] Optus Submission. Section 4.1.6, p.21.

[10] Defined in section 6 of the Telecommunications (Emergency Call Service) Determination 2019 (as made) dated 26 November 2019. Available at: https://www.legislation.gov.au/F2019L01509/asmade/text.

There were 18 recommendations[11] resulting from the Bean Review conducted following the November 2023 Optus incident. Of these, ten recommendations relate directly to new Triple Zero obligations. The list below sets out the status of our compliance uplift for each of these ten recommendations in relation to the new obligations.

- Initial amendments to the ECSD (effective 1 November 2024):
  - Rec#4: CSPs to warn users of BYO device limitations (*Compliant*)
  - Rec#A[12]: Block service to phones that cannot access TZ (*Compliant*)
- Subsequent amendments to the ECSD (effective 1 November 2025):
  - Rec#1: Wilting[13] and emergency camp-on functionality (*Compliant*)
  - Rec#3: Six monthly testing of end-to-end TZ ecosystem (*Compliant*)
  - Rec#5: Carriers to share real time outage information with ESOs (*Compliant*)
  - Rec#6: Outage reporting to the ACMA and DITRDCSA (*Compliant*)
  - Rec#7: Rationalise disruption protocol documents (*Not fully compliant*)
  - Rec#B: Change management plans for significant network changes that involve TZ (*Compliant*)
- The creation of C674:2025 Emergency Calling – Network and Mobile Phone Testing industry code[14]:
  - Rec#3: Six monthly testing of end-to-end TZ ecosystem (*Compliant*)
- Amendment to C536:2020 Emergency Call Services Requirements (Incorporating Variation No 1/2025)[15]:
  - Rec#16: Remote management continuity requirements for Carriers (*Compliant*)
- Telecommunications Legislation Amendment (Triple Zero Custodian and Emergency Calling Powers) Act 20255)[16]:
  - Rec#2: Establish a Triple Zero Custodian (*Compliant*)

As can be seen, Telstra is compliant with the ten recommendations except for one aspect of Recommendation#7 which requires carriers and CSP to notify customers about major outages in accordance with the CCO Standard.

Regarding the latter, we have been unable to identify a technically feasible way to meet the requirement in the CCO Standard to identify and notify all individual customers affected by a major outage in our network. The nature of these larger scale events prevents us from being able to determine (during the outage) which specific customers have been affected. Instead, Telstra has sought to address the intent of this obligation through developing a solution which enables customers to receive broadcast messages about major outages in the States or Territories that they choose. We have explained this situation to the Australian Communications and Media Authority and continue to liaise with them about it.

5 Outages of the Triple Zero ecosystem

Network outages, both planned and unplanned, cannot be completely eliminated. For this, and other reasons,[17] to give every opportunity to make a Triple Zero call when needed, global standards[18] include a

11 Inclusive of the two additional requirements added by the ACMA, namely “Rec#A” and “Rec#B”.

12 Recommendations #A and #B are additional requirements that were not in the original 18 recommendations arising from the Bean review

13 To prevent the base station providing any connectivity to a mobile phone via that base station.

14 C674:2025 Emergency Calling – Network and Mobile Phone Testing Industry Code, October 2025. Available at: https://www.austelco.org.au/wp-content/uploads/2025/10/C674-2025.pdf

15 C536:2020 Emergency Call Services Requirements (Incorporating Variation No 1/2025), October 2025. Available at: https://www.austelco.org.au/wp-content/uploads/2025/10/C536-2025.pdf

16 C536:2020 Emergency Call Services Requirements (Incorporating Variation No 1/2025), October 2025. Available at: https://www.austelco.org.au/wp-content/uploads/2025/10/C536-2025.pdf

17 For example, differences in coverage between competing mobile network operators.

18 3GPP standards.

"camp-on" mechanism that allows customers of one mobile network to use another mobile network to call Triple Zero, when their network is unavailable, including due to disruption. We also communicate with our customers ahead of any planned work, including upgrades, that require us to temporarily cease normal network operation. This allows our customers time to put in place alternative mechanisms to contact Triple Zero.

There are several scenarios where an emergency call may not reach the ECP. These include situations where the caller abandons the attempt before the call completes, where a caller is in marginal or intermittent network coverage, where a network outage prevents the call from progressing, or where device limitations or configuration issues interfere with connectivity. Each of these scenarios is distinct and highlights that call failures can occur within any part of the Triple Zero ecosystem.

This section of our submission starts with a brief description of work we have done to build resiliency into the Triple Zero ecosystem, followed by a description of an ECP incident that occurred in March 2024, and a reported matter that was not a Triple Zero incident in July 2025.

5.1 Building resilience across the Triple Zero ecosystem

Telstra has implemented a range of measures to strengthen the resilience of the ECS ecosystem to ensure continuity during disruptions. A key feature of this resilience is the diversity and redundancy built into the three ECP Call Centres that underpin the Triple Zero ecosystem. These call centres are geographically dispersed across Australia and operate on independent infrastructure, providing failover capability in the event of a localised outage. Each ECP Call Centre is equipped with diverse network connectivity and routing systems, ensuring that if one centre experiences an issue, calls can be seamlessly redirected to the others without service interruption.

Beyond physical diversity, we have invested in operational and technological improvements to further strengthen resilience. We have introduced real-time monitoring dashboards that track call volumes and system performance across all ECP Call Centres, and are augmenting these dashboards by the end of 2025 with to enhance our visibility of carrier-level and state-level traffic trends.

Automated load balancing ensures calls are distributed efficiently, and our welfare check escalation process alerts us when any dropped calls are detected.

The redundancy and diversity built into our network interconnect points and throughout our core network is designed to withstand outages and ensure that Triple Zero calls are carried to the ECP within strict service level targets.

We are also actively working with other carriers and ESOs on a project to introduce additional resilience for carrying emergency calls to and from the ECP. This initiative involves Telstra building an interconnection form the ECP to Optus and TPG that is completely independent of Telstra's core network, so emergency calls can continue to be delivered via that alternate connection in the (very unlikely) event that Telstra's core network is unavailable.

5.2 March 2024 incident

On 1 March 2024, an incident occurred where the ECP was unable to transfer 127 calls to ESOs. The incident lasted for 90 minutes, and was different to the Optus Incident, in that this was on the "downstream" side of the ECP (i.e., between the ECP and ESOs). Customers from all carriers and CSPs were equally impacted. The disruption, widely covered in the media, was triggered by a large spike in medical alert devices making unnecessary emergency registrations to Telstra's mobile network, which in turn triggered a latent software fault that resulted in two of the ECP databases becoming unresponsive and forcing the ECP to manually process the transfer of the calls.

Telstra has provided a full analysis of the cause of that incident, the effect of that incident, and how we dealt with, and recovered from, that incident. A report with more detail is available on our website.[19]

Following that incident, Telstra implemented additional monitoring layers to detect calling line identity (CLI) anomalies and database issues earlier.

Telstra has also worked with the ACMA to introduce changes in the latest version of the ECSD to provide the ECP and carriers with powers to control unnecessary emergency registrations to mobile networks from IoT devices like medical alert devices.

5.3 Reports of other incidents

On 5 July 2025, there was a reported disruption to the 106 emergency call relay service.[20] It is important to recognise that, during this disruption, no attempts were made by individuals to reach the 106 emergency call relay service, so no end users were impacted.

6 Roaming and Temporary Disaster Roaming

This section of our submission addresses item e) in the terms of reference for this inquiry.

> e) the limitations on domestic mobile telecommunications customers accessing services offered by alternate carriers, known as mobile phone 'roaming', which is particularly an issue in times of emergency in regional communities where mobile coverage can be less reliable;

We note this Committee is investigating matters related to Triple Zero. We note that neither roaming, nor Temporary Disaster Roaming (TDR), are required for a caller to access another mobile network for the purpose of making Triple Zero calls. The emergency camp-on function, embedded in global standards and implemented in all three primary mobile networks in Australia, allows any caller attempting to access the ECS, to "camp-on" to any other available network if their usual network is unavailable.

6.1 What is TDR, and how would it work?

Telstra and the industry, have investigated the feasibility of deploying a solution known as TDR. If implemented, TDR would enable mobile roaming between the mobile networks of the three MNOs within a declared localised area during emergencies or disasters in that area, for a short, specified duration.[21] For mobile customers in the disaster zone, this would mean that, even if the radio access component[22] of a mobile network is disrupted, TDR capability would allow them to stay connected using any other mobile

---

19 https://www.telstra.com.au/exchange/000-outage-report

20 Note: The 106 emergency relay service is separate to, and not part of the ECP.

21 Media Release, *Government to scope emergency mobile roaming capability during natural disasters*. The Hon Michelle Rowland MP and Senator The Hon Murray Watt. 23 October, 2023. Available at: https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/9433883/upload_binary/9433883.pdf

22 TDR is only capable of compensating for disruption of the radio access network and/or associated backhaul from a base station. If a mobile operator's core is disrupted, the ability to authenticate end users is lost, and as such, roaming (temporary or otherwise) will not work. TDR/roaming does not hand one MNO's customer base over to another operator; it simply provides access by allowing (foreign) customers onto another operator's network. This is the same as international roaming; when you leave Australia, you do not become the customer of an overseas operator; you remain the customer of the Australian MNO and simply use a foreign MNO's network to gain access. To become the customer of a foreign operator's network, you purchase a local SIM (e.g., prepaid) when you travel. A dual-SIM phone with two Australian SIMs is the internationally standardised mechanism to have access to multiple networks.

network in the area that is still working. In February 2024, Telstra conducted a successful TDR simulation to show that this is possible.[23]

While TDR is an innovative solution with the potential to provide temporary access to communications for regional and rural communities during disaster situations, there are several challenges to be managed. These include ensuring any surviving network is not overloaded from an influx of TDR traffic causing it to fail, which would be an even worse outcome for the impacted community.

Importantly, TDR will only work if there is participation by all of Australia's MNOs and appropriate support from government and emergency service stakeholders. We continue to engage with them on these matters. We are cognisant that satellite to mobile services will, in the near future, also improve the ability for customers to stay connected using their mobile devices even when the terrestrial network goes down (see section 6.2).

6.2 LEO Satellite services, UOMO and Emergency Calling

Low Earth Orbit (LEO) Satellite to Mobile (STM) services promise an exciting future of ubiquitous outdoor mobile connectivity, albeit more basic than terrestrial mobile. Telstra is already providing commercial LEO STM messaging (including SMS and iMessage) services to the Australian market.[24] We can expect LEO STM voice and then data to become available over time, as global standards mature, LEO STM satellite networks develop, suitable spectrum is assigned, STM voice technology is developed, and handsets capable of STM become widely available.

Despite this promising future, LEO STM technology is still nascent. The LEO STM ecosystem is currently based on proprietary modifications to network equipment using 4G standards, which can deliver limited LEO STM messaging only at this stage. We expect 5G standards in development to address these shortcomings, with devices capable of LEO STM services starting to become available from late 2027. We note that it is not currently possible to send an SMS to Triple Zero, and we would welcome the opportunity to continue working with the Government to develop this capability.

In February 2025, the Australian Government announced[25] it would expand the existing universal services framework to include a universal outdoor mobile obligation (UOMO). The Government subsequently consulted[26] on an exposure draft of a Bill to introduce UOMO, which closed on 19 October 2025. Telstra supports the intention of this obligation.

It is important to recognise the timeline for the advent of voice services over STM is dependent on mobile carriers gaining access to suitable spectrum,[27] satellite network capability becoming available to support voice, and most importantly, handset capability in accessing voice services over STM.

The Telecommunications (Emergency Call Services) Determination, 2025 requires that any carrier offering a public mobile telephone service (PMTS), must include capability to access the ECS (i.e. carry emergency calls). Thus, according to legislation, calls to Triple Zero will be made available when STM voice is introduced, or to put it another way, STM voice will not be introduced without the ability to call Triple Zero, because doing so would be in breach of carrier obligations under the ECSD.

---

23 Telstra Exchange. *Temporary Disaster Roaming: successful simulation shows what's possible*. 6 Feb 2024. https://www.telstra.com.au/exchange/telstra-temporary-disaster-roaming

24 Telstra Satellite Messaging is here. https://www.telstra.com.au/coverage-networks/mobile-technology/satellite-to-mobile

25 Universal Outdoor Mobile Obligation to improve outdoor mobile coverage across Australia. 26 February, 2025. https://www.infrastructure.gov.au/department/media/news/universal-outdoor-mobile-obligation-improve-outdoor-mobile-coverage-across-australia

26 See https://www.infrastructure.gov.au/have-your-say/consultation-universal-outdoor-mobile-obligation-uomo-draft-legislation

27 Spectrum that has been standardised by 3GPP for Non-Terrestrial Network (NTN) capability.

We look forward to continuing to work with the Australian Government on the introduction of STM voice services, in accordance with the UOMO legislation (once passed).

6.3 Mandated roaming is not required to access Triple Zero

As already noted, the emergency camp-on function, inherent in global standards and implemented in all three primary mobile networks in Australia, allows any caller attempting to access the ECS, to "camp-on" to any other network with coverage in the location they are calling from. Mandated roaming is not necessary for callers to reach Triple Zero.

We maintain that any requirements mandating particular forms of active mobile network sharing (such as roaming) would impair the incentive and ability of major investors, including Telstra, to improve regional Australia connectivity over the short, medium and long term. Telstra does not support mandated roaming as it undermines competitive differentiation and reduces investment. A more detailed explanation of our position can be found in section 2.4.4 of our submission to the 2024 Regional Telecommunications Review.[28]

7 Consumer device compliance

Item c) iii) of the terms of reference requires the Committee to explore the adequacy of regulatory, legislative and policy frameworks governing access to the ECS.

> c) iii) the adequacy of regulatory, legislative and policy frameworks governing Australians' access to emergency telecommunications assistance including whole-of-government responsibilities and co-ordination and the protection of vulnerable Australians;

This section of our submission explores at a high level, the complexity inherent in the technology options for accessing the ECS, the regulations that govern consumer devices to ensure their ability to reliably access the ECS regardless of the situation, and what can be done to tighten enforcement of regulations to reduce the risk of Australians having a device that would not be able to access the ECS in all situations.

Reliable access to the ECS is, in large part, predicated on a mobile device's capabilities across a range of technology options, and that the device will behave in a predictable manner. Importantly, some of the settings governing the access to various technology options (e.g., 3G/4G/5G, VoWiFi, and in the future, STM voice) can depend on carrier settings loaded into the device based on the SIM inserted into the device (e.g., a Telstra SIM).

The increasing capability of consumer devices,[29] along with their customisation for different markets globally and increasing complexity, can result in a wide range of bespoke device configurations. These configurations can manifest as rules in the device to select only a 3G network over which to place emergency calls, or restrictions preventing use of Voice over Wi-Fi (VoWiFi) networks to place emergency calls even when compatible Wi-Fi networks[30] are available.

---

28 See Telstra's submission to the 2024 RTR, section 2.4.4, p.56. Available at: https://www.rtirc.gov.au/submissions

29 Two examples are Voice over Wi-Fi (VoWiFi) calling, and ability to access satellites.

30 Not all Wi-Fi networks are compatible, and therefore capable of carrying VoWiFi. For example, VoWiFi is not allowed in some Wi-Fi networks such as enterprise Wi-Fi networks.

7.1 Methods for mobile users to access Triple Zero

There are several methods mobile devices can use today to make emergency calls to the ECP. In the future, STM voice will be another method. Note: our comments below concern methods to access Triple Zero from a mobile device; they do not cover calls from fixed-line devices.[31]

- **"On-net" emergency calls** (including locked screen calls): This is the most common case. There is a Telstra SIM in the phone, and the phone is inside Telstra's terrestrial coverage. Regardless of whether the device is screen-locked or not, the device will attempt the call. Telstra supports voice calls across all radio frequency bands (except mmWave bands), and the device needs to select the band it will use for voice.
- **SIMless or other MNO ("foreign") SIM ECS calls**: These calls are from devices that have no SIM, or the SIM of another network operator, and the device is inside Telstra's terrestrial coverage. In this case, the phone will camp-on to our network, and we will carry the emergency call to the ECP over our network.
- **Camp-on to another network (Telstra SIM)**: If a device, with a Telstra SIM in it, is not within coverage of our network but is in the coverage of another network,[32] the device will camp-on to the other network (regardless of whether screen-lock is on or not).[33] Importantly in this scenario, the device is presented with a range of radio frequency bands from two other mobile networks (depending on location). The device generally looks to find the strongest signal (across all the radio frequency bands), and depending on the device's capabilities, looks for 4G or possibly 5G networks first, and failing that, looks for 3G or 2G networks (known as Circuit Switched Fall Back, "CSFB"[34]).
- **Voice over Wi-Fi (VoWiFi)**: VoWiFi refers to mobile phone voice calls made over IP networks using Wi-Fi, instead of over the mobile (cellular) network.[35] This capability dates back to 2008 and is common in most mobile phones manufactured this decade. Telstra and device vendors began progressively introducing VoWiFi from the middle of last decade,[36] supporting VoWiFi calling across a range of network types including NBN (both fixed and satellite), and more recently, over Starlink fixed broadband services.[37]
- **Forthcoming STM Voice**: In the future (2-3 years from now), we expect to support voice services over our STM network (STM voice). Under the ECSD, STM voice is required to include access to the ECS from when it is first offered.

When attempting to make a call, including to Emergency Calls, the call may fail for a large variety of reasons including congestion, loss of signal, or a network software error. When this failure occurs, the network will either send an error code (if it is capable) or simply not respond to the device to indicate the call failure. In response, the device will take action by trying alternate options. In the extreme circumstance of a catastrophic network failure, the device should camp-on to another network to make the 000 call. However, there is significant complexity behind this. There are numerous failure scenarios, yet only a finite number of error codes defined in the standards. Given the same error code could be

---

31 While we do not cover fixed-line calling to Triple Zero, we note that our Smart-Modem gateway devices used in conjunction with an NBN service will fail-over to our mobile network when there is an outage in the NBN.

32 For example, some in-building coverage where other networks are repeated inside the building but Telstra's is not, or when Telstra's network is disrupted due to planned maintenance or unplanned outage events.

33 Recently, we discovered an issue where some older Samsung devices do not camp-on to TPG's network, because the devices are configured to only use a third generation (3G) network when attempting to access the ECS over TPG's network. See: https://www.telstra.com.au/exchange/older-mobile-devices-calling-triple-zero-

34 3GPP Technical Specification TS 23.272. Circuit Switched (CS) fallback in Evolved Packet System (EPS). Version 18.0.0 for Release 18 is available at https://www.etsi.org/deliver/etsi_ts/123200_123299/123272/18.00.00_60/ts_123272v180000p.pdf

35 GSMA. Voice over Wi-Fi. https://www.gsma.com/solutions-and-impact/technologies/networks/ip_services/vowifi/

36 For example, see the introduction of VoWiFi on Apple iPhones, 10 May 2017. https://www.smh.com.au/technology/telstra-brings-wifi-calling-to-iphones-20170510-gw1ctb.html

37 Telstra Satellite Broadband using Starlink: https://www.telstra.com.au/small-business/internet/starlink

used for “everyday” failures as well as a catastrophic failure, the interplay between the network and devices is not straightforward.

To be clear, we’re not saying the level of complexity is beyond the capabilities of a device. What we are saying is due to the level of complexity, we should expect different behaviour across devices because different device manufacturers will code the sequence in which it moves through the various options differently. Some manufacturers will preference low-band frequencies first, while others will preference mid-band frequencies. Some will preference circuit-switched fallback (CSFB), which allows devices on a 4G network to make or receive voice calls by temporarily falling back to an older network like 3G, before VoWiFi. We are not yet sure how STM voice will be prioritised.

It is important to recognise that working through each option to access the ECS takes a finite amount of time. For example, if a device preferences CSFB over VoWiFi, then after being unsuccessful in placing an emergency call over a 4G network (e.g., outside terrestrial coverage, or the mobile network is disrupted), the device will then scan for a 3G network on every known frequency, before attempting to make the call using VoWiFi. It could take tens of seconds to sequentially work through each band from each carrier looking for a 3G network, before the device moves on from exploring CSFB options to moving to Wi-Fi.

As such, in network disruption scenarios, it can take 60 seconds or more for a device to explore options, and eventually try options like VoWiFi. Many callers, especially in anxious situations such as an emergency, abandon the call attempt well before the device has exhausted all options.

7.2 Recent issues with older Samsung handsets

Recently, we discovered[38] an issue with certain older Samsung handsets failing to properly camp-on to TPG's mobile network to place an emergency call. While these handsets are capable of placing emergency calls over the Telstra and Optus networks, the manufacturer’s configuration in the handsets forces the device to only use 3G when using TPG’s network, and they are therefore unable to make emergency calls on TPG’s network.

Upon confirming this issue, we notified both Optus, TPG and Samsung, and began taking steps to alert our customers in accordance with the ECSD obligations, including contacting customers to advise them to either replace or update the software on their phone (where possible), and posting information on our website. For customers in vulnerable circumstances, such as financial hardship, we provided replacement phones free of charge.

38 To identify this issue, we obtained an early model J-series device and created a simulated environment where only TPG’s network was available. We created the simulated environment in a fully Radio-Frequency (RF) shielded room, where we used a mobile repeater configured to only repeat TPG’s network, such that in this shielded room, only TPG’s network was available (i.e., in the room Telstra’s and Optus’ networks were “down”). We put a Telstra SIM in the Samsung device, and attempted an emergency (test) call, which was unsuccessful.