OPTUS

Submission to the Senate Standing Committee on Environment and Communications

Triple Zero service outage

November 2025

Executive Summary

Optus acknowledges the serious and tragic nature of the events of 18 September 2025 (the 2025 outage), when a technical failure during a network upgrade impacted 605[1] unique service numbers connecting to emergency services in South Australia, Western Australia, the Northern Territory and far west New South Wales.

This incident has been linked to the fatalities of people who sought help and who were unable to immediately reach emergency services. We extend our deepest sympathies to their families and friends. Optus apologises to them and to all those who sought help that day but could not access it.

Optus accepts accountability for its failures that led to this interruption of Triple Zero services. As one of Australia's major telecommunications providers, we understand that maintaining uninterrupted access to emergency calls is fundamental to public safety and community confidence.

Following the outage, Optus moved to implement changes to strengthen its change control, internal escalation and incident management processes, particularly within its contact centres and network operations teams, to ensure that processes are followed and, in particular, that any future reports of issues affecting emergency calls are rapidly identified and escalated. As part of Optus' transformation program work is underway to on-shore network operations functions and some critical customer care functions, and these plans have been accelerated.

An independent review, led by Dr Kerry Schott AO, was immediately commissioned by the Optus Board to identify the technical, operational and governance factors involved, recommend measures to prevent recurrence, review compliance with Bean Review recommendations and review incident response and notification processes. Optus has also appointed Kearney, a leading global consulting firm, to begin immediate oversight, quality assurance and verification as Optus uplifts its mobile network management, processes and services consistent with required standards.

Optus is cooperating fully with the Australian Communications and Media Authority (the ACMA), the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the Department), and other relevant authorities, and is determined to engage constructively with key stakeholders on opportunities for improvements to its own operations and processes, as well as the structure and operation of telecommunication networks in Australia more broadly.

The 2025 outage occurred in a regulatory environment that had already undergone significant reform following the 2023 Optus outage and the post-incident review lead by Mr Richard Bean (the Bean Review).

Despite improvements implemented since that time, the 2025 outage shows that further action is required by industry and government to collaboratively ensure the resilience of the Triple Zero ecosystem in light of further information about the operation of emergency calling.

[1] The breakdown of impacted services is provided in more detail in section 4.1.6

Optus provides this submission to the Senate Standing Committee on Environment and Communications in that spirit: to give a transparent account of what occurred, to outline the immediate and longer-term steps being taken to strengthen our systems, and to provide the relevant background and contextual information to support a clear understanding of this incident and how recurrence can be prevented. A timeline of key events based on Optus' investigations to date is included as Appendix A.

The submission is structured as follows:

1. About Optus
2. The Optus Network
3. Triple Zero ecosystem
4. The 2025 outage
5. Background: 2023 Optus outage
6. Optus transformation program
7. Conclusion

Through this submission and willing participation with the Senate Standing References Committee on Environment and Communications, as well as the ACMA and Optus' internal reviews, Optus is determined to demonstrate its ongoing commitment to learning from this failure and ensuring that the Optus network is as robust and reliable as it can be to support the vital communications needs of Australians into the future.

1. About Optus

1.1 History

Optus commenced operations in 1992, breaking the existing monopoly and, for the first time, bringing Australians choice in telecommunications providers. In that same year, Optus acquired AUSSAT and became Australia's first non-government satellite operator.

The introduction of competition in the sector has resulted in significant investment and innovation, benefiting all Australians. Deregulation in the telecommunications market also saw a revolution in mobile communication variety and pricing.

In 2000, Optus was the first Australian company to allow SMS between carriers; in 2008, Optus launched the first iPhone in Australia; and in 2012, Optus launched its 4G network followed by the launch of its 5G network in 2019. This was the same year that Optus completed the world's first 5G data call over 2300MHz spectrum and flew Australia's first 5G drone.

In 2024, Optus announced its regional network-sharing agreement with TPG Telecom to increase regional coverage and accelerate the 5G rollout leading to the launch of the Optus 5G+ network in February 2025. Expansion of the network footprint continues with 2,520 5G+ sites planned for delivery by the end of 2031 – filing 245 coverage blackspots in regional communities and major roads.

Optus also brought competition to the cable television market in Australia as well as in the sports content market, through the launch of Optus Vision in 1994 and Optus Sport in 2016.

With more than 40 years of operations in space from the beginnings of AUSSAT, Optus has launched 11 geosynchronous satellites providing broadcast, military communications and telecommunications services to a wide range of government agencies and commercial organisations. In 2003, Optus launched its C1 satellite to support the Department of Defence with the largest hybrid communications and military satellite ever launched in Australia. In 2014, the Optus 10 satellite was launched, now carrying a range of broadcasting services including Foxtel and the Viewer Access Television Service (VAST) to remote and very remote Australia.

In more than 30 years of operation, Optus has brought competition, choice, value and innovation to the Australian telecommunications market. Last calendar year Optus contributed $5.2 billion to the Australian economy and supported 12,700 jobs.

1.2 Optus services

Optus delivers more than 12 million services operating in each state and territory across Australia. The connectivity powered by Optus enables:

- home internet
- mobile telephony
- business and enterprise ICT and connectivity services
- payment system enablement
- satellite television and radio; and
- fibre optic infrastructure management

Optus' mobile network covers 98.5 per cent of the population with 9525 total mobile network sites. Since the 3G network switch-off in late 2024, Optus has repurposed spectrum to boost the capacity, speed, and reliability of its 4G network to ensure more Australian have access to faster speeds, lower latency and improved connectivity.

To support enhanced coverage in remote and regional Australia, Optus has successfully partnered with the Commonwealth and state/territory governments to improve connectivity outcomes, supporting the delivery of mobile connectivity for the first time. This includes through co-funding arrangements such as the Commonwealth Government's Mobile Black Spot Program.

Optus provides and manages approximately 36,000 kilometres of high-speed fibre optic connectivity nationally, of which over 10,000 kilometres of fibre backbone links Australia's capital cities.

Since 1985, Optus has been Australia's primary satellite provider, launching 10 satellites, operating 13 spacecraft, and providing support to over 100 international space programs. Optus Satellite provides Australia with a vital onshore and sovereign capability, particularly supporting Defence military satellite communication requirements and delivering an unrivalled television and radio services backbone via the Viewer Access Television Service (VAST). These services are delivered from Optus main satellite operations centre at Belrose, NSW, supported by backup ground stations in Lockridge, WA; Hume, ACT; and Regency Park, SA. From these stations, Optus undertakes continuous satellite network monitoring, video, voice and data delivery, support and troubleshooting across a range of industries.

Optus serves a diverse range of customers across the country, including major contracts with small businesses, corporates, and government departments through Optus Enterprise. As a trusted partner-of-choice delivering critical and secure telecommunication and IT services, these services range from high-performance network solutions to cloud-based tools, AI automated solutions and managed ICT services. As part of Optus Enterprise, a wide range of services is provided to government departments and agencies across Australia – from voice and mobile services to ICT managed services, data management and other contracted communications services.

Optus is also heavily involved in programs to protect and assist Australians online. Optus has introduced anti-scam measures blocking more than 570 million scam calls and 260 million SMS since December 2020 and supporting reduced fraud losses by more than 80% through multi-factor authentication.

Since 2013, Optus has been operating one of the longest running digital safety and wellbeing education programs to school students, and since 2019 Optus has also been delivering its Donate Your Data program which provides internet access to disadvantaged Australians. This digital inclusion program has assisted more than 53,000 people and delivered over $30 million in value.

1.3 Corporate structure and governance arrangements

Singtel Optus Pty Limited (Optus) is the operating parent of the Optus business, which is ultimately wholly owned by Singtel Telecommunications Limited (Singtel).

Optus is an Australian incorporated company subject to Australian Corporations law and relevant local regulation.

Optus has a separate Board consisting of seven directors: two executive directors (Optus Chief Executive Officer, Mr Stephen Rue and Optus Chief Financial Officer, Mr Michael Venter), four non-executive directors (Mr John Arthur – Chairman, Mr Nicky Tan, Ms Michaela Browning and Mr Andrew Parker) and Singtel Group Chief Executive Officer, Mr Yuen Kuan Moon. The Optus executive management team is based in Australia.

The Optus Board operates independently and within various group policies, as is usual in group corporate structures. It is responsible for the overall direction, strategy, management, performance and oversight of the Optus group and meets at least eight times per year.

Optus has always had a Board in place, with functions delegated to various committees. However, in recent years, Singtel has adopted a stronger 'op-co' model where the Boards of key component businesses are far more empowered to make their own decisions, oversee their own local operations and be accountable for performance and operations. This has coincided with increasing the size of the Board and number of non-executive directors.

In 2024, the Optus Board also established Board committees to further support its governance and oversight of the Optus business:

- Audit Committee (Chair, Mr Parker)
- Risk Committee (Chair, Mr Tan)
- Human Capital Committee (Chair, Mr Arthur)

These committees are scheduled to meet quarterly, but meet more frequently when required.

Additionally, the Optus Defence and Satellite Committee (Chair, Ms Browning) and Executive and Strategy Committee (Chair, Mr Yuen) meet as required.

Each committee has its own charter, which is reviewed periodically, which outlines the role and accountability of the committee and deals with procedural matters.

The Optus Defence and Satellite Committee was established to deal with defence matters, and its charter confirms (in keeping with Optus' obligations to the Department of Defence) that all defence material is only seen or handled by Australian citizens, who must not be employees or directors of Singtel.

Optus' governance structure ensures the Optus Board makes key decisions on strategy and operations (including procurement) and maintains oversight of and accountability for performance and operations. While a limited number of matters are reserved to the Singtel Board (such as M&A transactions over SG$300 million, combined Singtel/Optus procurement, appointment of external auditors for Singtel Group accounts), the Optus Board is fully empowered to manage Optus' affairs.

Following the 2025 outage, the Board established two further committees (the Response Oversight Committee and the Expenditure Approval Committee) to oversee Optus' response to the outage, the progress of the Independent Review, to be conducted by Dr Kerry Schott AO, which the Board has commissioned and to oversee and approve the changes Optus is accelerating in its program of transformation.

1.4 Investment in Australia and economic contribution

Australians expect communications services to be affordable, resilient and secure. Optus shares those expectations and for more than 30 years we've worked to meet them by connecting Australians through mobile, fixed and satellite networks.

In recent years, Optus invests an average of around $1.4 billion on capital spending each year on improving and growing our Australian network. This investment covers both ongoing operations and network improvements, supporting reliability and resilience across the country.

More broadly, since 1992 Optus has contributed approximately $79 billion to the Australian economy. This includes cumulative investment of $56 billion in infrastructure and the payment of $4.3 billion in spectrum fees to the Commonwealth Government.

Last calendar year, Optus' contribution to the Australian economy was more than $5.2 billion, supporting 12,700 jobs. It predicted that $19 billion will be added to the economy by 2030 via Optus 5G+ services, creating 6,800 new jobs and enhancing productivity for business across the country.

Various engagement initiatives also support local communities. In the last financial year, Optus contributed $28 million to the Australian community via community organisations and sponsorships and our people contributed over 16,400 volunteering hours to charities and causes close to their heart. The Optus Digital Thumbprint program has educated 710,000 students in schools across Australia on topics spanning Gen AI, cyberbullying and scams. This includes 50,000 students in 2025 alone.

With the support of Commonwealth and state governments, Optus also supports enhanced connectivity outcomes in regional, remote and very remote communities through co-funding partnerships to deploy new mobile solutions. Since 2016, Optus has received grant funding from the Mobile Black Spot Program, a Commonwealth Government initiative designed to reduce known coverage black spots across Australia. Optus has contributed more than $105 million through several rounds of the program and received almost $196 million from the Commonwealth to address coverage gaps in the mobile network.

Optus is a lead supporter of the Mobile Network Hardening Program, a Commonwealth Government co-funding program designed to enhance mobile network resilience through funding for backup power generation, battery supply, solar cell installation or mobile tower relocation away from high-risk locations. Since the beginning of the program, Optus has contributed more than $11 million to co-funding measures and received over $23 million to deliver resilience infrastructure around Australia.

2. The Optus Network

2.1 Structure and architecture

Optus operates within a highly complex and interconnected telecommunications ecosystem, involving thousands of towers, exchanges, fibre links, satellite services, and core network components. The network also relies on trusted global partners and industry-standard technologies, with resilience depending on collaboration across vendors, regulators, government, and competitors.

All these elements must work seamlessly to deliver reliable connectivity.

2.1.1 How a call is connected

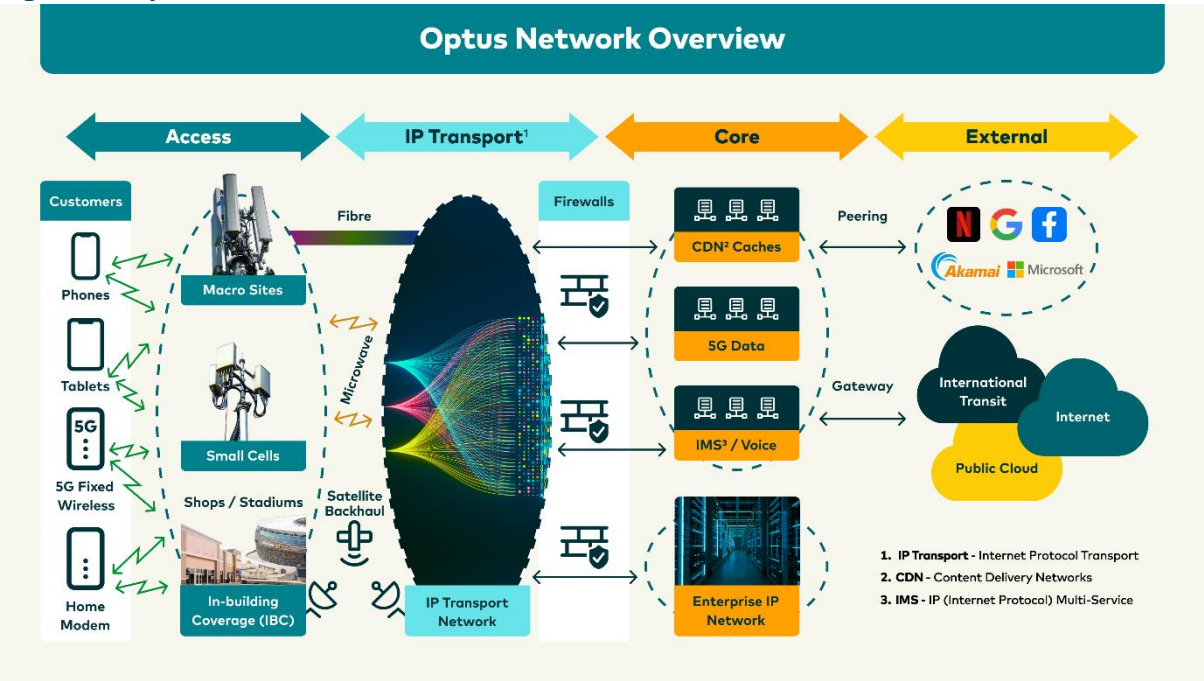
The equipment and network infrastructures involved in a mobile phone call include:

- the user's device
- mobile towers and base stations
- fibre, microwave and satellite linkages
- IP networks
- exchanges and data centres
- the core network
- network interfaces within Optus, towards other network operators and internationally.

When an Optus customer makes a mobile phone call, their phone connects to the nearest and strongest 4G mobile base station (5G towers handle data only). The call is then transmitted to Optus' core network via fibre, microwave or satellite linkages to an exchange and then onto a destination core network – either Optus or another operator in Australia or overseas.

This process continues in reverse to the recipient's handset.

Figure 1 – Optus network overview



2.1.2 Key network components

- **Access**: Provides wireless connectivity between user devices and the Optus mobile network (via mobile towers)
- **IP (Internet Protocol) Transport**: National transmission & IP network enabling traffic exchange between access networks, core platforms and external networks
- **Core**: Provides for authentication, accounting, routing and supervision for all services
- **Enterprise IP Network**: Dedicated network platform for providing fixed enterprise connectivity services to small and medium business and corporate customers
- **International Transit**: Optus has international transit via exchanges outside of Australia

Optus operates 9,525 mobile sites and 19 network exchanges across Australia.

A **network exchange** is a physical building or facility where call or data traffic is routed to different locations within a telecommunications network.

A **core** is a mobile network's central infrastructure, managing and processing the calls and data services from the mobile towers and is typically housed in a network exchange.

2.1.3 Vendor management

Optus employs a multi-vendor strategy to mitigate risks across our network. Our major vendor partners are Nokia and Ericsson.

Vendor selection is based on technical suitability, compatibility, and strategic considerations. Integration is managed through contained environment testing, ongoing monitoring and robust contract governance. Our multi-vendor strategy mitigates risk through diversification and fosters innovation by leveraging competition. This approach avoids dependency on a single supplier, ensuring stronger long-term partnerships, continuous improvement, and network evolution.

Optus has a robust contract and vendor governance process in place for our strategic vendors. Supply contracts include key deliverables and Critical Service Levels / Key Performance Indicators which are assessed and reported on a monthly basis.

For our strategic vendors (including Nokia and Ericsson), governance forums include quarterly executive business reviews, monthly steering/program group meetings where delivery and performance is discussed and improvement plans agreed, and regular commercial/contractual meetings to address contractual changes, disputes and other risk related matters. Optus has also entered into tri-party Dispute Avoidance Board agreements for our key supply contracts, where an independent Dispute Avoidance Board Member supports both parties to resolve issues and concerns collaboratively prior to formal disputes arising.

A comprehensive vendor scorecard is produced to support discussion at the quarterly executive business review.

Testing is conducted for every significant network change, especially when integrating new equipment from different vendors. These tests are conducted in contained environments prior to introduction into a live operational setting.

2.2 Network outages and faults

The Optus network on average achieves a network uptime of 99.26%. Over the last quarter (July-September 2025), the Optus network achieved a network uptime of 99.45% – this accounts for planned and unplanned outages. This is comparable with network performance across European mobile network operators.

2.2.1 Typical network fault issues

Outages are temporary and are generally planned (associated with scheduled maintenance or upgrades), or occasionally they are related to damage to infrastructure or other unplanned events, such as severe weather.

The main categories of unplanned fault issues are:

- **Power Failures**: Loss of mains electricity – typically from major energy providers – is the leading cause of mobile network service disruptions, particularly during natural disasters. When outages exceed the backup capacity of onsite batteries, mobile tower sites may experience service interruptions.

  To mitigate this risk, Optus protects sites via battery back-up and proactively deploys generators to affected sites where the estimated time to restore grid electricity surpasses battery endurance thresholds. This approach ensures continuity of service and reinforces our commitment to network resilience under adverse conditions. Optus also deploys a range of other resilience infrastructure (including satellite backhaul mobile base stations) to provide temporary coverage or offset loss of permanent coverage solutions.

- **Hardware Failures**: Faults in network equipment such as base station components (power infrastructure, air conditioners, routers, plug-in units, etc.), core network nodes (plug-in units, fan units, routers, etc.), or transmission hardware (plug-in units, fibre optic systems that facilitate data flow between network sites, etc.) can cause service interruptions.

  Optus maintains layered redundancy across its infrastructure to minimise customer impact including automated failover protocols, real-time fault detection and escalation and strategic hardware replacement cycles. These measures ensure rapid response and uphold service reliability across the national footprint.

- **Third-Party Supplied Transmission**: Issues with transmission links provided by external vendors or partners can also result in network faults. These can be as a result of fibre cuts, power failures or hardware failures in a third-party provider's networks outside the control of Optus. Traffic is automatically rerouted in the event of most fibre cuts to ensure minimal disruption to customer services and supports rapid recovery.

- **Change related incidents**: Optus typically executes between 3,000 to 4,000 changes across the network per month. Optus continues to strengthen the change management process to minimise or mitigate any change related incidents.

From 30 June 2025 to 11 October 2025 in accordance with the definitions under the Outage Standard, Optus has recorded:

Significant Local Outages – 332

- Regional – 240 (two of these were later determined to have occurred in metro areas and should not have been triggered as regional local outages)
- Remote – 90
- Major Outages – 0

In accordance with the Emergency Call Services Determination (ECS), there has been one Significant Network Outage (SNO) in this same period (18 September 2025).

2.2.2 Alerts and monitoring

Optus operates a Network Service Experience Team (NSET) located in the Network Operations Centre, which operates 24 hours a day, seven days a week. This team's role includes monitoring various aspects of the operation and performance of Optus' services, including the call drop rate and call setup failure volumes for voice calls generally, as well as for emergency calls to the emergency call service specifically.

2.3 Network resilience measures

In most cases, Optus mobile towers are reliant on electricity supply provided through the national grid. While in most cases mains electricity supply is sufficient to provide a continuous stable network connection, unexpected power interruptions in power supplies can take a mobile tower offline.

To address this, Optus invests heavily in a range of resilience measures designed to ensure continuity of service to our customers until mains power can be restored. These include:

- **Fixed Batteries**: Optus has installed short to medium-term fixed duration batteries at all mobile tower sites across Australia to support minor/short mains power supply outages.

- **Fixed Generators**: Over 200 fixed generators have been installed at the most vulnerable base stations across Australia. These include several ‘hub locations’ where other towers are reliant on the hub for their operation.

- **Portable Generators**: A significant number of portable generators can be deployed to critical sites as needed. Optus will often pre-deploy portable generators to areas of natural disaster risk ahead of major weather events to best ensure continuity of service.

- **Portable Fuel Pods**: Situated adjacent to fixed generators, Portable Fuel Pods can be deployed to extend generator supply by up to five days beyond the generator’s own fuel supply.

- **Critical Power eXtender Batteries**: These high-voltage longer life batteries support service continuity across mobile sites during power failures.

- **Battery Resilience Program**: Optus has an ongoing battery enhancement program that ensures batteries are optimised and replaced rapidly where required.

- **Satellite Backhaul Mobile Base Stations (SatCats)**: Optus operates a fleet of independently powered satellite connected mobile base stations. These are easy to deploy during natural disasters, offering high bandwidth and 4G/Wi-Fi connectivity.

- **COW (Cell on Wheels)**: Optus operates a fleet of COWs that, when deployed, provide a longer-term temporary solution with better coverage and high capacity than a Satcat. The transmission backhaul access is provided via microwave or fibre-based transmission and takes longer to mobilise, configure and set up.

- **Rapid Deployable Coverage**: Solutions for emergency evacuation centres and temporary mini sites.

2.4 Notification processes for planned network upgrades and unplanned network outages

In cases of planned network impacts, customers who spend a significant amount of time in the impacted area are notified of work being done.

These notifications are provided to both mobile and NBN customers. An initial notification is sent to inform customers about an upcoming network upgrade in their area – this typically occurs in the days leading up to a planned outage. These notifications are sent via email or SMS depending on customer contact preferences. Further communication is provided to customers at the conclusion of the planned work if completed as scheduled.

In the event planned upgrades take longer than anticipated, an extension notification is sent to customers. These notifications are also sent via email or SMS depending on customer contact preferences. On average, Optus sends around 700,000 unique notifications to customers per month. Specifically for planned mobile interruptions, notifications are sent to both primary account holders (where their registered address is within an interruption footprint) and service holders in the impacted area (where a customer is within the area of an interruption at the time of notification). For NBN services, it is sent only to the account holder as per their registered address.

For unplanned outages that meet the criteria for Significant Local Outage or Major Outage (see table below) under the *Telecommunications (Customer Communications for Outages) Industry Standard 2024*, who Optus must notify depends on the cause of the outage and size of the outage. As soon as practicable, Optus must always:

- notify external stakeholders (including the ACMA);

- notify carriers or service providers with whom we have a commercial arrangement and whose end-users are impacted by the outage; and

- update our public facing website.

Where a Significant Local Outage or Major Outage is not caused by a natural disaster, Optus must directly notify end-users (for example via SMS, email or app). This includes residential, small business, and enterprise and business customers. For Major Outages not caused by a natural disaster, Optus must also proactively notify media and communicate on social media.

Outage notifications are initiated when Optus either detects an outage meeting the Significant Local Outage or Major Outage criteria for its network or receives notification from another carrier that they are experiencing a notifiable outage that is impacting Optus customers. The notifications required under the Outage Standard relate to outages where customers are unable to establish and maintain a relevant carriage service, such as a mobile telecommunications service, and excludes impacts on over-the-top services, such as streaming services, or Internet of Things data-only services.

As part of the latest variation to the ECS Determination, from 1 November 2025 Optus will be notifying emergency services organisations in the relevant state or territory where a Major Outage or Significant Local Outage is occurring where the carriage of emergency calls is impacted.

In situations where calls to emergency services are impacted, but this impact does not meet the threshold for a Significant Local Outage or Major Outage notification, Optus has implemented a voluntary manual process to ensure swift email notification and accurate information is provided to external stakeholders (the ACMA and the Department), the Emergency Call Person (ECP) and relevant Emergency Service Organisations (ESOs).

Prior to 1 November 2025, the regulations also included a process for a Significant Network Outage with different thresholds. The 2025 outage triggered a notification under the Significant Network Outage protocol instead of the Significant Local Outage or Major Outage protocols referenced above.

Table 1 – Regulated notification processes

Significant Local Outage (*commenced 30 June 2025)*	Assessment is completed based on profiled impacted customers and thresholds set out in regulations (including Remote 250 customers ≥3 hours actual or expected duration and Regional 1,000 customers ≥6 hours actual or expected duration). Communications required to customers and external stakeholders (including the ACMA, the Department and ESOs that have opted in) plus public facing website. (*NB: Notifications will be required to ESOs in the state/territory where an outage is occurring from 1 November 2025*). Communications must include the key information required under the regulations (location, size of impact, cause, impacted services, estimated time for resolution, next update cycle) to the extent known at the time of the communication. The cause of an outage is not required to be disclosed if this is likely to raise national security or network security concerns. Communications are provided to stakeholders in alignment with required communication cycles, including a public facing website until outage is resolved, once every six hours for first 24 hours and once every 24 hours thereafter noting any material change will also be provided out of cycle if applicable. Final resolution communication is sent to stakeholders listed above and website is updated.

Major Outage (*commenced 31 December 2024*)	Assessment is completed based on profiled impacted customers and thresholds set out in regulations (including 100,000 customers or a whole state or territory ≥1 hour actual or expected duration). Communications required to customers & external stakeholders (including the ACMA, the Department and ESOs that have opted in) plus public facing website. (*NB: Notifications will be to all relevant ESOs from 1 November 2025*). Communications must include the key information required under the regulations (location, size of impact, cause, impacted services, estimated time for resolution, next update cycle). The cause of an outage is not required to be disclosed if this is likely to raise national security or network security concerns. Communications are provided to stakeholders in alignment with required communication cycles, including public facing website until outage is resolved, once every six hours for first 24 hours and once every 24 hours thereafter. Noting any material change will also be provided out of cycle if applicable. Final resolution communication is sent to all stakeholders (as above) and website is updated.
Significant Network Outage (*ceases 31 October 2025*)	Significant Network Outage defined as an unscheduled network failure that adversely affects the carriage of emergency calls over that network in a significant way, having regard to the number of customers impacted by the outage, the likely time to restore the service and the availability of other carriage services that can be used to make and receive calls. The thresholds for these criteria are determined by the individual carrier. Communications required to the ECP, the ACMA and other carriers or carriage service providers who use that network for telecommunications services.

3. Triple Zero ecosystem

3.1 Overview of the Triple Zero ecosystem

The Commonwealth sets out aspects of the legal framework for emergency calls (000, 112 and 106) under the *Telecommunications Act 1997* and the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (the TCPSS Act).

These Acts are supplemented by various other regulatory instruments and co-regulatory documents, which impose obligations on carriers, carriage service providers and the ECP relating to tasks such as managing outages, customer complaints, stakeholder notifications, welfare checks, and set out technical requirements for how networks should carry calls and location information.

These instruments include:

- *Telecommunications (Emergency Call Service) Determination 2019*
- *Telecommunications (Customer Communications for Outages) Industry Standard 2024*
- *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*
- C536:2020 *Emergency Call Service Requirements Industry Code*
- C674:2025 *Emergency Calling – Network & Mobile Phone Testing Industry Code*
- G557:2025 *Location Information for Emergency Calls Industry Guideline*

These requirements are in addition to global technical standards set for both network operators and device manufacturers, for example by the European Telecommunications Standards Institute (ETSI) or the Third Generation Partnership Project (3GPP), which also influence emergency call service arrangements. The aim of these international standards is to ensure interoperability in different jurisdictions.

Telstra, under a contract with the Commonwealth Government, serves as the ECP for calls to Triple Zero (000 and 112). Telstra then redirects those calls to the relevant ESO in each state or territory. The ECP function for emergency calls to 106 from TTY devices (teletypewriter devices for people who are deaf, have a hearing or speech impairment) is operated by Concentrix as part of the National Relay Service. In Victoria, the ECP will forward calls to Triple Zero Victoria who handle the call-taking and dispatch for emergency services.

The large number of participants (telcos, the ECPs and the ESOs) contributes to the complexity of the end-to-end of the ecosystem, especially when taking into account that some parts of the ecosystem involve oversight from the Commonwealth, and other parts involve the states and territories who manage their jurisdiction's relevant emergency services (police, fire and ambulance services).

Optus is a member of various industry associations, committees and working groups. These work to enhance the effectiveness of the Triple Zero ecosystem. These bodies focus on improving resiliency, facilitating cooperation between stakeholders, developing rules and technical specifications and proposing new initiatives to ensure emergency responses meet changing technology and community expectations. These groups include:

- the National Emergency Communications Working Group Australia/New Zealand (NECWG), which has members from across the Triple Zero ecosystem as well as government and regulator representatives;
- the Triple Zero Coordination Committee (TZCC), operated by the Department, with a representative from each state and territory and a carrier representative present at each meeting; and
- working committees under the auspices of the Australian Telecommunications Alliance (ATA), the telecommunications industry peak body responsible for co-regulatory codes and guidance documents.

We note that NECWG has recently released a White Paper[2] outlining some of the current challenges for the Triple Zero ecosystem and recommendations to address these, including accelerating the establishment of national governance and consultation mechanisms for Triple Zero services, the development of a National Emergency Contact Strategy to address changes in the way the community communicates, identifying options for increasing efficiency in the Triple Zero operating model, the creation of consistent regulatory guidelines for emerging technologies and the designation of key emergency infrastructure as critical assets.

3.2 Triple Zero ecosystem operation during mobile network outages

The ability to access the emergency call service is critical and all handsets with or without a SIM must be able to access the emergency call service on any operator network where there is a mobile signal. Supporting access to the emergency call service across any operator network requires additional capabilities over and above normal voice calling, which is designed to be primarily supported via their own network.

There are several technical solutions in place to facilitate an emergency call to connect during mobile network outages such as the emergency camp-on process, and base station wilting.

3.2.1 Emergency Camp-on

Emergency calls will first be attempted on the customer's network. If the emergency call cannot be established on the customer's network, the emergency camp-on process is triggered.

The emergency camp-on process operates such that the mobile devices attempt to search for all available networks and attempt to make an emergency call once connecting to an available network. The timeframe to complete the emergency camp-on process varies but can be between ~40 to 60 seconds or more and some customers may end the call before the emergency camp-on process completes. This variability in emergency camp-on performance is a known issue within industry and requires an industry-wide response.

We observe that devices behave differently during the emergency camp-on reselection process. This is due to mobile device providers adopting different implementations of the emergency call handling process for non-standard network scenarios. This is because the 3GPP standards that apply to devices do not mandate specific device behaviour during non-standard network scenarios.

3.2.2 Wilting

The *Telecommunications (Emergency Call Service) Amendment Determination 2025 (No.1)* comes into effect on 1 November 2025 and requires carriers to 'wilt' a mobile base station in the event it loses connectivity to the core network.

Wilting is the intentional shutdown of a mobile base station when it loses connectivity to its core network and cannot carry emergency calls. This shutdown triggers mobile devices in the area to emergency camp-on to another available mobile network that *can* carry emergency calls. This process seeks to ensure that customers can still make an emergency call even if their own network is unavailable.

[2] Available at: https://necwg-anz.org/wp-content/uploads/2025/10/Emergency-Communications-in-Australia-a-NECWG-White-Paper.pdf

When there are failures deep inside the core network, as opposed to between the base station and the core network, wilting is not automatically triggered, and would need to be manually triggered.

In a Multi-Operator Core Network (MOCN) scenario where connectivity is only lost to one mobile operator core network, the corresponding network ID (Public Land Mobile Network ID - PLMN) for the mobile operator that has lost connectivity to the core will stop being broadcast, while the alternate PLMN will continue to be broadcast, and will therefore be able to carry emergency calls, including emergency camp-on calls.

3.3 Challenges with the current Triple Zero ecosystem architecture

As noted above, the Triple Zero ecosystem is complex, with a large number of participants nationally, who work in parallel to ensure our communities can get the help they need when they need it. There is broad acknowledgement across all participants in the ecosystem (including industry, government and the ACMA) that aspects of the Triple Zero system require continued improvement, with the current focus areas relating particularly to device compatibility, emergency camp-on behaviour, and end-to-end network interoperability under outage conditions.

It is important to note, however, that these challenges are on the "uphill" side of Triple Zero – i.e. connecting a customer call via their carrier to the ECP. Challenges also exist on the "downhill" path – from ECP to the ESOs, which must be part of the solution. (See, for example, the NECWG White Paper referenced above for more details).

Following the Bean Review recommendations, and resulting regulatory changes, the Australian Telecommunications Alliance has worked with carriers to develop updated industry codes, including for a new testing framework to better understand how different handsets and networks perform when making emergency calls, including in emergency camp-on scenarios. The C674:2025 *Emergency Calling – Network and Mobile Phone Testing Industry* Code has recently been registered by the ACMA, and the first round of testing is due to commence with the test facility engaged by the Department for this purpose.

Optus and the other mobile network operators are participating in ongoing coordinated efforts with government and the regulator to identify, test and address known issues as they arise, and to strengthen the overall resilience and reliability of the Triple Zero service. We look forward to contributing further to these efforts.

Significant work is also underway by Optus to enhance our internal testing regimes, and to work closely with the ECP to enhance Triple Zero testing arrangements, to enable more frequent, automated tests to be carried out in a way which does not interfere or adversely impact the actual Triple Zero environment. We appreciate Telstra's engagement in, and support of this work, as we work together to ensure more robust emergency call services for our communities.

4. The 2025 outage

4.1 Description of outage and its cause

4.1.1 General background

On Thursday 18 September 2025, Optus experienced a network outage that lasted over 14 hours from 00:17 AEST to 14:34 AEST (the 2025 outage). During this period, 605 unique service numbers attempting to make Triple Zero calls were unsuccessful in connecting to emergency services in South Australia, Western Australia, the Northern Territory and parts of far west New South Wales. All other mobile and fixed voice and data services continued to operate normally during the Triple Zero outage; it was emergency calls that were impacted.

Preparatory work for a firewall upgrade at the Regency Park exchange in South Australia had commenced in early September 2025.

This was part of a broader program that began in April 2025 to update DMZ firewalls (production traffic firewalls) and IX firewalls (network management firewalls) across multiple states. All of the DMZ production firewalls had been upgraded successfully. At the time of the outage, six IX firewalls were upgraded successfully, and the Regency Park exchange IX firewall was the seventh firewall to be upgraded.

During that work on Thursday 18 September 2025, a "soft lock/hard lock" change to a specific piece of network infrastructure known as a session border gateway (SBG) was performed without redirecting traffic off the platform prior to applying the soft lock. A “soft lock” is a procedure that stops new calls from being established but allows established calls to continue. A “hard lock” forcibly terminates all active call sessions and blocks the initiation of any new connections. Where a lock is applied, the correct process is to first redirect the traffic at the SBG before applying the lock.

When the change above was implemented, voice traffic continued to be directed to the SBG but failed to be routed through the SBG as it had not been redirected. This meant that calls were not able to be processed through that part of the network.

Normal voice calls contain two exchange addresses and as a result automatically redirected to other exchanges in the network. These normal voice calls were not impacted. Customer calls to Triple Zero behave differently. When the Regency Park SBG was locked, Triple Zero calls attempting to pass through the Regency Park SBG were not successful. The next steps following that call depended on a number of factors. In some cases, Triple Zero calls "camped-on" to other networks or were connected through another exchange in the Optus network. In other cases, Triple Zero calls were unsuccessful due to other factors. (See sections 4.1.5 and 4.1.6).

4.1.2 Process and interaction with Nokia

Optus owned and operated the relevant Controlled Networks and Controlled Facilities. Optus and Nokia Solutions and Networks Australia Pty Ltd (Nokia) have contractual arrangements in relation to incident management and change control procedures. Optus is accountable for its Controlled Networks and Controlled Facilities and has contracted certain services to Nokia under these arrangements.

Discussions regarding the Regency Park IX firewall upgrade took place between 3 September and 17 September 2025. During this time Optus and Nokia engaged in a planning and approval process for the firewall upgrade.

A project meeting with the platform owners to review the scope of changes and discuss impact assessments was held on 8 September. Some of the required members of the Optus core networks engineering team were not present at the meeting.

As part of this change process, the instruction sent by Optus to Nokia indicated that a lock should be applied to infrastructure known as the SBG prior to the upgrade being implemented. Optus did not expressly request that traffic be offloaded from the Evolved Packet Gateway (EPG) prior to the lock being applied, however this activity is included in the correct Method of Procedure.

During the process of planning the upgrade, an outdated Method of Procedure document was selected for the implementation of the upgrade by Nokia personnel and was peer-reviewed by three Nokia personnel. The Method of Procedure did not include making changes in the EPG to "offload" traffic from the SBG prior to implementing the change to lock the SBG.

The Method of Procedure that Optus expected Nokia to use, and which had been previously used at this site for a DMZ firewall, did have the step of offloading traffic from the SBG prior to implementing the change to lock the SBG. The procedure used on all successful IX firewall upgrades previously had no locks, and thus no offloads or diversions. The change to be implemented was marked by Nokia personnel as an escalated (or urgent) change and with a zero-risk level. This rating of risk and urgency was incorrect and meant that the change did not go through an Optus risk and engineering assessment which involved a review by senior Optus engineers. As this review step did not take place, the Method of Procedure used by Nokia was not reviewed with Optus prior to the change.

Nokia's implementation of the change process commenced at about 00:00 AEST on 18 September 2025, in preparation for the firewall upgrade scheduled for 19 September 2025. This was using the incorrect Method of Procedure, and was conducted 24 hours earlier than originally planned, with the SBG changes brought forward to 18 September 2025. It appears this may have been done by Nokia to provide Nokia with further time to conduct the firewall upgrade on the following night.

A network "soft lock", which drains the traffic and prevents new traffic entering the SBG was put in place at 00:17:27 AEST on 18 September 2025. This procedure is part of a managed (planned) shutdown procedure or planned change. The outage commenced at this time due to the traffic not first being offloaded off the SBG device. Optus identified that the first call attempt which did not connect to Triple Zero occurred at 00:18:07 AEST on 18 September 2025.

4.1.3 Alerts: internal

A spike was observed by a Nokia engineer in VoLTE[3] Key Performance Indicator (KPI) performance graphs, used to visualise representations of KPIs for monitoring and assessing the health of VoLTE services. These graphs identified general voice call failures on the bypassed network element. An incident ticket was then raised by Nokia within Optus' systems for attention by Nokia at 00:20:16 AEST on 18 September 2025.

[3] VoLTE: Voice Over LTE

Subsequently, automated emails were generated which contained links to near real-time graphs in Optus' monitoring systems indicating higher call setup failure rates, call drop rates, call registration failure rates and interface call setup failure rates. These graphs highlight call failures on the bypassed network element that were not specific to Triple Zero. These automated emails were reviewed by an Optus engineer. A further incident ticket was raised by Optus at 00:47:33 AEST on 18 September 2025.

At 00:53 AEST on 18 September 2025, Optus further contacted Nokia at its command centre (which handles major incidents) through Microsoft Teams highlighting the incident. At 00:56 AEST on 18 September 2025 there was a response from Nokia's command centre indicating that the incident was due to the then-ongoing change. The incident tickets were then investigated by a Nokia engineer who informed Optus that the activity which caused the alerts was due to ongoing activity related to the change.

At about 02:10 AEST on 18 September 2025, a hard lock was executed on the SBG, which configures the SBG to reject any registration attempts until the lock is removed. This action forcibly terminates all active sessions and blocks the initiation of any new connections. It is typically employed when a node is taken offline for updates, fault isolation, or other operational requirements.

Post change checks were completed by a Nokia engineer at around 02:40 AEST on 18 September 2025. The check did not lead to the identification of the issue with Triple Zero calls.

4.1.4 Alerts: Inbound customer and emergency service calls

During the 2025 outage, five inbound customer calls were made to Optus contact centres reporting difficulty reaching Triple Zero. The procedure for dealing with such calls is to ask if there is an immediate danger. If the answer is affirmative, the call is put through to the ECP. None of the five callers were in immediate danger. These calls were not appropriately escalated internally.

For one customer, the Optus contact centre provided the contact details for the Norwood store and suggested that the customer attend the store in person due to the urgency. The customer subsequently attended an Optus store at around 13:23 AEST on 18 September 2025 and purchased a new phone, having stated that their phone was old and not functioning properly.

The Optus Call Centre in Manila received a customer call advising they were not able to contact Triple Zero at 10:13 AEST on 18 September 2025. Additional calls were received that same day by the Optus Call Centre from other Optus mobile customers informing Optus that they were not able to contact Triple Zero at 10:47 AEST, 11:37 AEST, 12:57 AEST and 14:11 AEST.

Optus received a call from the South Australian Ambulance Service at 13:15 AEST asking whether there was a known issue with Triple Zero operability. At 13:17 AEST, Optus received a second call from the South Australian Ambulance Service in which they notified Optus of an issue with Triple Zero operability. At 13:25 AEST, Optus received a third call from the South Australian Ambulance Service to inform Optus that the South Australian Police had set up a ‘bridge call’ relating to the issues and requested an update on the outage.

At 13:53 AEST on 18 September 2025, the South Australian Police called the Optus Networks Emergency Services Support team, operated in Australia on Optus' premises by Nokia, and reported that they had been receiving calls from ambulance services regarding Triple Zero calls not working.

4.1.5 Emergency camp-on

During the outage, some devices successfully made a Triple Zero call on the Optus network, some devices camped onto other networks, and some devices were not successful in connecting to Triple Zero (see section 4.1.6 below).

Emergency camp-on success may have been dependent upon network characteristics, device configuration and the time it took for the device to connect. Optus observed that some specific devices were able to successfully emergency camp-on to other networks for some customers, but other customers with the same devices did not connect to Triple Zero based on the length of time it took the device to connect. This suggests that the outcome was also dependent on whether the call was ended before the emergency camp-on process could complete.

Optus considers its network is generally comparable to other Australian networks except in relation to particular timer settings. Optus is currently investigating the extent to which timer settings had any impact in this outage, as explained below. Further work is also ongoing in relation to device behaviour as certain devices searched for 3G connectivity during the outage where the primary connection was not successful. This device behaviour also appears to be a factor in unsuccessful calls to Triple Zero during the outage and may have broader implications.

In relation to timer settings, Optus' ongoing investigation relates to whether the interaction between its timer settings and particular device behaviours may have impacted whether the calls were able to connect to Triple Zero, particularly through another part of the Optus network. Initial indications from that investigation are that:

- The inactivity timer for Optus' EPG SOS dedicated bearer is set at 10 seconds. Based on Optus' current investigations, where the SBG is locked without redirecting voice traffic from the EPG, if a device handset is unable to connect to the SBG in the 10 second period, the session between the device and the EPG will be disconnected. The call attempt does not fail, but this will cause the device to enter into its (device-specific) emergency calling failover behaviour, which may involve attempting to search for a 3G network and/or another 4G network to camp-on. The 10 second timer had been set in 2022, following engagement with the ACMA and Ericsson (which supplied the EPG infrastructure), to address an issue with certain Google Pixel phones repeatedly failing to make emergency calls.

- When the SBG was locked without redirecting voice traffic from the EPG, the EPG SOS inactivity timer may have resulted in some handsets being disconnected from the EPG before attempting to connect to another SBG on the Optus network (a secondary approach). Some devices did connect to Triple Zero via a secondary approach during the outage.

- The time taken for a device to attempt a secondary approach is device dependent.

- Not all devices are configured to attempt a secondary approach.

- It appears that devices impacted by this issue (i.e. which did not attempt a secondary approach) would still have followed device failover settings to search for a 3G network and/or attempt to camp-on to another 4G network, and may have succeeded in reaching Triple Zero.

Optus is continuing to investigate this issue and engaging with Ericsson to determine the optimum inactivity time setting for the EPG. Further work is also ongoing in relation to device behaviour which also appears to be a factor in unsuccessful calls to Triple Zero during the outage and may have broader implications.

4.1.6 Number of unique service numbers during outage

Optus has previously communicated that there were 631 unique service numbers whose Triple Zero calls were potentially impacted by the outage. This was based on a conservatively estimated outage end time of 15:00 AEST on 18 September 2025. Subsequently, it was determined that for the period of the outage based on the end time of 14:34 AEST there were 605 unique service numbers[4] whose Triple Zero calls were potentially impacted.

Of these 605 unique service numbers:

- 150 unique service numbers had successful Triple Zero calls:
  - 65 of these connected through another Optus exchange either on the first call or within a short time of the first call attempt;
  - 19 unique service numbers were ultimately successful in connecting to Triple Zero after delay; and
  - 66 connected through emergency camp-on to other networks.

- 455 unique service numbers appear not to have connected to Triple Zero.

4.1.7 Identification and rectification of outage

Optus identified the outage at about 13:17 AEST on 18 September 2025, following the call from the South Australian Ambulance Service referred to in section 4.1.4.

Optus and Nokia then commenced investigating the cause of the outage.

At 14:16 AEST a senior Optus engineer requested another engineer to investigate whether the firewall upgrade process was the cause of the outage. The instruction to remove the lock was given on an incident call at about 14:20 AEST and the system command to commence the unlock process was given at 14:23 AEST. The node impacting Triple Zero traffic began unlocking at 14:29 AEST on 18 September 2025 and finished at 14:31 AEST on 18 September 2025.

The impact of unlocking the SBG at Regency Park restored normal service, which was tested and confirmed (verification testing confirming successful call routing through the Telstra ECP) at 14:34 AEST.

Since the 2025 outage additional controls have been implemented in the change management process, including greater operational oversight, including:

- Mandatory pre- and post-change testing for Triple Zero call routing during any network upgrade.

- Daily Triple Zero test calls across all states and territories to verify connectivity.

[4] For completeness, some of the 605 service numbers were used internally by Optus staff to test connectivity to Triple Zero and were not calls by individuals seeking emergency assistance.

- Real-time monitoring and alerting for emergency call traffic, with escalation protocols to our new Critical Services Team.
- Enhanced change management protocols, including stricter approval processes and rollback procedures.
- State-based Triple Zero New alarms and manual escalation pathways to ensure fallback systems engage when needed.
- Acceleration of onshoring program commenced earlier in 2025 to return network operation, network monitoring and customer care support functions to Australia.

These matters are also being comprehensively reviewed under the Independent Review commissioned by the Optus Board and led by Dr Kerry Schott AO.

4.2 Customer and public engagement

4.2.1 Welfare checks of impacted customers

Once Triple Zero connectivity was restored in the afternoon of 18 September, Optus commenced a process to identify and contact customers whose calls to emergency services may not have connected during the outage. This process, known as a welfare check, is conducted to ensure customers welfare is identified and is a process required under section 28 of the *Telecommunications (Emergency Call Service) Determination 2019*.

Optus has an established process in place for conducting welfare checks. In line with other providers, Optus' standard welfare check process is conducted via outbound phone calls or text messages (SMS). In this instance, Optus made welfare checks by outbound phone calls rather than SMS because the legacy SMS Hub system had been decommissioned.

In a welfare check, customers are asked if they need assistance. If the answer is yes, their details are forwarded to the police for a formal welfare check. If they don't need assistance, no further action is taken. Where customers cannot be reached, Optus refers those cases to state/territory police for follow-up, in accordance with established procedures.

At 14:29 AEST on 18 September 2025, Optus' networks team initially estimated there were 10 unsuccessful Triple Zero calls in South Australia and Western Australia. However, following the initial internal investigation it became known that 10 unsuccessful Triple Zero calls occurred between 12:00 AEST and 13:00 AEST. No impacted individuals were identified at this point. Optus initiated the welfare check process at this time by instructing Nokia to provide Optus the Call Detail Records (CDRs) that related to the outage. CDRs are typically obtained from the core network.

At 15:48 AEST, Nokia provided Optus with the CDRs which showed no unsuccessful calls. The technical nature of the fault meant that unsuccessful Triple Zero calls were not captured in the data, as the calls did not reach the part of the core network from which the records are usually obtained. This is because call setup failed prior to the establishment of Session Initiation Protocol signaling, used to initiate, manage and terminate real-time multimedia communication sessions (VoLTE calls) over IP networks. This meant that the use of CDRs in this instance did not identify the unsuccessful Triple Zero calls.

The engineering team was then required to develop a new method to identify and extract unsuccessful Triple Zero calls. This process was both complex and time intensive, involving multiple iterations and refinements to accurately identify the affected customers. The key steps undertaken are described below.

- At about 16:05 AEST, Optus completed a call trace in an effort to identify the unsuccessful Triple Zero calls. The call trace in this instance did not identify the unsuccessful Triple Zero calls. Optus continued to investigate the availability of data.

- From about 18:30 AEST, Optus then undertook further deep dive investigation of Optus devices that could capture the data. At about 19:05 AEST, Optus commenced work to attempt to capture the potentially affected Triple Zero calls from its internal systems. This was not an established process, and this took some time to filter through large amounts of data.

- At about 19:50 AEST, the first 100 impacted service numbers were identified through the analysis of data extracted from the internal systems using source data from the Radio Access Network (RAN).

- From about 20:00 AEST, Optus continued work on refining its process and identifying the remaining unsuccessful Triple Zero calls. This work involved reviewing emergency call bearer information.

- The first 100 welfare checks commenced at 20:34 AEST and were concluded at 21:33 AEST (with data relating to unsuccessful checks subsequently being provided to police between 22:57 and 23:04 AEST on 18 September 2025).

- At 23:38 AEST, Optus identified a further 524 potentially impacted service numbers based on a search for unsuccessful calls over the period between 00:30 AEST on 18 September 2025 and 15:00 AEST on 18 September 2025, subject to validation checks.

- The list of these further 524 service numbers was discussed at an Optus networks team meeting which took place at 06:00 AEST on 19 September 2025. It was determined at this meeting that further validation of the additional service numbers was required. That validation was then undertaken up to 09:00 AEST the same morning.

- After an Optus Crisis Management Team meeting at 09:00 AEST on 19 September 2025, at about 10:00 AEST the list of further impacted service numbers was sent to the contact centre for welfare checks to be undertaken.

- Optus then undertook further preparation, briefing and additional training of staff. The additional 524 welfare checks commenced at 12:04 AEST on 19 September 2025 and were concluded at about 14:00 AEST on the same day. Data relating to unsuccessful checks was subsequently provided to police between 16:41 AEST and 16:48 AEST on 19 September 2025.

- From about 12:00 AEST on 21 September 2025, Optus conducted additional reviews of data to check the numbers of impacted service numbers produced. As a result of this review, at about 12:20 AEST on 22 September 2025, a further 7 impacted service numbers were identified. These service numbers were impacted in the period between the

commencement of the outage and 00:30 AEST on 18 September 2025, which was not within the original search parameters based on Optus' then understanding of the time period of the outage.

- The further 7 welfare checks commenced at 13:58 AEST on 22 September 2025 and were concluded at 14:14 AEST on the same day (with data relating to unsuccessful checks subsequently being provided to police at 14:23 AEST on 22 September 2025).

4.2.2 Customer communications

Optus did not send a direct notification message to each of the customers affected or likely to be affected by the outage. The outage did not fall within *the Telecommunications (Customer Communications for Outages) Industry Standard 2024*.

For completeness, Optus notified impacted customers through Optus' publicly available website, app, Facebook account and national media channels.

4.2.3 Public communications

With the emergency call network operating again and the immediate public risk removed, Optus continued to gather information to understand exactly what had happened and the impact before making public statements. At that stage, system data indicated a small number of affected calls and no information regarding loss of life. As additional data was analysed overnight and welfare checks were conducted, that understanding changed significantly.

Optus executives progressively became aware of two fatalities linked to the outage through the morning of Friday 19 September. At that stage, however, all welfare checks had not been completed. Optus executives wanted to ensure that when the Optus CEO contacted the Commonwealth Government, the regulator and addressed the Australian public via media with as much information as possible.

As the welfare checks continued, Optus learned of another fatality at 12:40 AEST on Friday afternoon. Still at that point, Optus did not know what further welfare checks might reveal. These welfare checks were completed at 14:00 AEST and Optus compiled and validated all information. At 14:36 AEST, the Optus CEO contacted the ACMA Chair. This was the first information to the ACMA that the issue was much more serious than indicated in notifications on 18 September, and it was the first time Optus informed the regulator that fatalities had occurred.

An Optus Board meeting regarding the outage was held from 15:00-15:35 AEST. In parallel and throughout the afternoon there were numerous contacts with state police, the Department, and the Minister for Communication's office (the Minister's Office). At 16:36 AEST, Optus sent an invitation for a media conference which commenced at 17:45 AEST.

A press release was issued in conjunction with the press conference and Optus conducted extensive media engagement to provide the public with information as understood at the time. A second press conference took place at 15:20 AEST on 20 September with a press release issued shortly after.

Further media statements were issued on 20 September, 21 September, 22 September, 24 September and 30 September, along with additional press conferences on 21 September and 24 September. These can be accessed via the Optus website at:
https://www.optus.com.au/notices/triple-zero-call-failures-update

4.3 Compliance with regulatory notification obligations

The 2025 outage did not fall within the scope for notifications in the *Telecommunications (Customer Communications for Outages) Industry Standard 2024*, as normal calls were still able to be made. Within the definitions of the Standard, no Significant Local Outage or Major Outage occurred and the obligation to notify Relevant Stakeholders under the *Telecommunications (Customer Communications for Outages) Industry Standard 2024* was not triggered.

The relevant obligation applies only where an outage results in an end-user being unable to maintain a relevant carriage service (amongst other things), as this is a mandatory limb of each of the definitions of Major Outage and Significant Local Outage under that Standard. Despite the outage, Optus customers were still able to establish and maintain the relevant carriage service as non-Triple Zero calls were not impacted. An emergency call is not in and of itself a carriage service (being defined in the *Telecommunications Act 1997* as "*a service for carrying communications by means of guided and/or unguided electromagnetic energy*"); rather, the end-user uses an underlying carriage service to make the call. On this basis, no Significant Local Outage or Major Outage (within the definitions in the Standard) occurred.

Optus did however treat the outage as a Significant Network Outage under the *Telecommunications (Emergency Call Service) Determination 2019*. The required notifications for an Significant Network Outage are to the ECPs (also sent to the ACMA consistent with the then requirements of Industry Code C536:2020), and these were sent firstly as a text to the Telstra ECP at 14:19 AEST and then from 15:17 AEST via emails to the ACMA, the ECP for 106 (Concentrix) and then the ECP for 000 and 112 (Telstra).

Following that text message via SMS, a Significant Network Outage notification was given by Optus via email at 15:17 AEST advising that Optus had become aware of a Significant Network Outage in South Australia, Western Australia and the Northern Territory that adversely affected the carriage of emergency calls over the Optus network before handover to the ECP. That email included, among other recipients, the following relevant stakeholders ECP for 106 (emergencycontact@relayservice.com.au); and ACMA (emergencycallservices@acma.gov.au).

The notification was also intended to be sent to the ECP for 000 and 112 (Telstra ECP) at the same time. At 15:18 AEST Optus called the Telstra ECP to confirm they had received the 15:17 AEST email. A typographical error in the email address was identified which meant that the original email had not been delivered to the intended recipient, Telstra ECP, and the notification was re-sent to the correct email address (imotriplezerosupport@team.telstra.com) at 15:26 AEST.

The ACMA has since commenced an investigation into Optus's compliance with emergency call service regulations and other related rules. Optus is cooperating with that investigation.

4.4 Government and emergency service organisations engagement

Stakeholders such the Department and Minister's office are not required to be notified of a Significant Network Outage. Nevertheless, Optus undertook additional notifications to several

stakeholders. As these voluntary notifications were part of ongoing stakeholder engagement, rather than a regulatory requirement, this activity was led by Optus' government relations team.

Between 19 and 21 September, Optus maintained contact with the Minister's office. Optus first attempted to contact the Minister's office via phone call at 14:31 AEST on 18 September, less than an hour after the issue was first identified and escalated internally. That call was returned at 14:34 AEST. Emails providing written notice of the 2025 outage were then sent at 14:45 AEST stating that Triple Zero services had been affected and at 14:52 AEST, advising that connectivity had been restored.

These emails also included correspondence to an email address at the Department that had previously been used for mandatory notifications and continues to be used by the Department as a centralised inbox for correspondence. At that stage, Optus had early information that 10 calls to Triple Zero had been impacted. Welfare checks had not commenced, and Optus was not aware of any fatalities.

Between 19 and 21 September, Optus maintained regular communication with the Minister's office, providing more than 20 updates as the scope of the incident became clearer. Additionally, on at 14:36 AEST on 19 September 2025, the Optus CEO called the Chair of the ACMA to discuss the outage. Optus also informed the Telecommunications Industry Ombudsman (TIO) about the outage by telephone at about 18:30 AEST on 19 September 2025.

From 18 September, Optus' regulatory team frequently engaged with state and territory ESOs. Optus acted as the key liaison and escalation point for these queries, keeping agencies informed as more information on the outage came to light.

Optus communicated directly with impacted agencies to inform them of the outcome of the welfare checks, including when Optus became aware of the tragic loss of lives. Between 18 to 21 September, Optus remained in constant contact with ESOs to provide further status updates.

4.5 Optus response to the 2025 outage

Optus acknowledges that the failures that led to – and followed – the 2025 Triple Zero outage were unacceptable. Optus apologises to all those who sought help that day but could not rely on Optus to access that help. The company has taken immediate steps to strengthen the resilience of its network and improve internal escalation processes to ensure faster communication with regulators, government and emergency services.

We accept that further work is needed to improve within Optus and at an industry level to enhance the Triple Zero ecosystem so that such incidents like this can be avoided, whichever carrier is delivering the service.

We have already undertaken a number of actions to enhance monitoring and escalation of Triple Zero call failures and implement compulsory escalation procedures.

We are committed to building stronger systems and better safeguards and working with all stakeholders to undertake critical reform.

We accept we have more work to do to continue to transform the business, strengthen the Optus network, and restore the confidence and trust of the Australian public. We will listen, learn and commit ourselves to earn back confidence through action (See section 6).

4.5.1 Technical and network assurance measures

From a technical and network assurance perspective, Optus has taken the following actions:

- Introduced enhanced 24/7 monitoring of Triple Zero call volumes and failure rates at a state and territory level down to SA3 to enable early detection of anomalies or deviations from normal call traffic.

- Implemented daily Triple Zero test calls in every state and territory, pending industry-wide work on automated end-to-end testing.

- Worked with vendors to ensure that all firewall and core network changes mandatorily require multi-layer approval and validation by the Network Operations Centre before implementation.

- Further, Optus has commenced a technical review of network redundancy and emergency call routing systems with independent oversight from Kearney, a leading global consultancy, to confirm compliance with all applicable standards and to strengthen resilience.

4.5.2 Operational, process and escalation improvements

Optus acknowledges there were serious process issues in the failure to escalate the customer reports of Triple Zero outages. The way these customer calls were handled was not acceptable. Since identifying these missteps, Optus has taken some immediate actions, including removing some service representatives from the Optus account effective immediately.

In addition, the following actions have been taken:

- Implemented additional processes in Optus call centres to support customers who are unable to call Triple Zero. This includes an additional compulsory escalation process following any customer reports of Triple Zero failure, ensuring concerns are referred to the networks team, so they can investigate promptly.

- Made our onshore Critical Services Team a direct escalation point for all Optus Contact Centres and front-line Optus staff for incidents reporting to be impacting critical services.

- Ensured the network reporting process now includes daily calls to Triple Zero before and after any upgrades to test performance.

- Strengthened coordination between network operations and regulatory compliance teams to ensure immediate internal escalation and external notification when emergency call issues arise.

4.5.3 Communication and government relations measures

Optus has taken the following actions:

- Implemented new verification procedures for all manual notifications to government and regulators, including cross-checks of recipient addresses and multi-recipient confirmation for every manual email.

- Expanded the distribution list for outage notifications to include multiple contacts across the Department, Minister's office, and the ACMA.

4.6 Future improvements planned by Optus

The Optus Board has appointed Kearney, a leading global consulting firm, to begin immediate oversight, quality assurance and verification as Optus uplifts its mobile network management, processes and services consistent with required standards. During the performance of their work, Kearney will report regularly directly to the Optus CEO and Board.

In addition to the actions already taken, Dr Kerry Schott AO has been appointed by the Optus Board to lead an Independent Review into the 2025 outage. The Independent Review will look at the causes of the 2025 outage, how Triple Zero calls are managed, and how Optus responded. It is expected to be completed before the end of the year, and Optus has committed to releasing the findings publicly.

Optus is fully cooperating with the ACMA as it investigates both the technical causes of the 2025 outage and compliance with regulatory obligations.

Optus also welcomes the Senate Inquiry process as an important opportunity to contribute to industry-wide lessons on resilience and public safety. In parallel, Optus is working collaboratively with the Department, the ECP (Telstra), and other major carriers including Telstra and TPG, consistent with the joint industry statement reaffirming a shared commitment to ensuring that the Triple Zero system continues to meet the critical needs of Australians.

5. Background: 2023 Optus outage

In 2023, Optus experienced a national network outage impacting customers across Australia. Shortly following the outage, Optus conducted a rigorous post-incident analysis to identify what occurred and the root cause of the outage – the following information was shared with the Senate Standing Committee on Environment and Communications as part of the Inquiry into the 2023 outage.
The 2023 outage is not connected or associated with the Triple Zero outage of 18 September 2025 – both incidents were the result of different circumstances and materially different root causes.

At around 04:05 AEDT on 8 November 2023, the Optus Network Operations Centre observed a loss of connectivity affecting our consumer core network. This resulted in a loss of consumer fixed and mobile services, and some enterprise services. Enterprise broadband services were not impacted as these operate via a different core network infrastructure.

In the initial stages of the outage, Optus prioritised the restoration of services as soon as possible, which required re-establishing connectivity to key elements of the network. The following information and detail regarding the sequence of events was collated subsequent to restoration.

The outage occurred due to more than 100 devices automatically self-isolating in order to protect themselves from an overload of IP routing information. These self-protection limits are default settings provided by the global equipment vendor who provided the equipment to Optus (Cisco).

This unexpected overload of IP routing information occurred after a software upgrade at one of the Singtel internet exchanges (known as STiX) in North America, which is part of the wider Optus international network. During the upgrade, the Optus network received changes in routing

information from an alternate Singtel peering router, which then propagated through multiple layers of our core network. As a result, at around 04:05 AEDT, the pre-set safety limits on a significant number of Optus network routers were exceeded. Although the software upgrade resulted in the change in routing information, it was not the cause of the 2023 outage.

Restoration required a large-scale effort across more than 100 devices in 14 sites nationwide to facilitate the recovery (site by site). This recovery was performed remotely and also required physical access to several sites.

At the time of the 2023 outage, the behaviour of the network that led to the impact on services was unclear. Several hypotheses and paths to restoration were explored over the period up to 10:30 AEDT.

Through this process, Optus identified that resetting routing connectivity addressed the loss of network services. This occurred at 10:21 AEDT and the following work then commenced:

1. Resetting and clearing routing connectivity on network elements which had disconnected themselves from the network.

2. Physically rebooting and reconnecting some network elements to restore connectivity.

3. Carefully and methodically re-introducing traffic onto the mobile data and voice core to avoid a signalling surge on the network.

The steps that resolved the incident were actioned across multiple (more than 100) network elements and various geographic locations nationally. Simultaneously, over the course of the morning, it was also important for Optus to investigate and rule out any indication the outage was caused by malicious actors.

Optus consumer internet services and DNS information started to come back online from 10:38. Optus technicians continued to progressively restore the impacted routers, including routers used for mobile services with 99.72% of RAN sites restored by 15:30 AEDT.
Approximately 150 engineers, technicians and field technicians were in the core group of personnel working on resolution. That core group was augmented by 250 additional personnel, providing further support and monitoring. We also worked with five leading international vendors who assisted us with resolution and advice.

Although 99.72% of RAN sites were restored by 15:30 AEDT, Optus declared the network outage closed at 16:00 AEDT.

The restoration of the network to provide connectivity for our customers was at all times our priority. Following the formal resolution of the outage at 16:00 AEDT, the team closely monitored the performance of the network and continued to review the circumstances regarding the outage to make any necessary changes to further increase the resiliency of the network. This work continued throughout the remainder of the week, through the weekend, and until the afternoon of Monday 13 November 2023.

5.1 Measures taken since the 2023 Optus outage

As referenced above, Optus immediately commenced a post-incident review of the 2023 outage and conducted investigations to determine root cause, identify further vulnerabilities and make changes to network operations.

Optus initiated a multi-phase program to further strengthen network resiliency.

- **Phase 1** – focused on immediate recovery and stabilisation on the day of the 2023 outage;
- **Phase 2** – from November 2023 to March 2024 performed comprehensive reviews and application of critical learnings; and
- **Phase 3** – implemented a strategic network resilience program.

To prevent a recurrence of a future network incident similar to the 2023 outage, two enhancements were made to the network:

- The configuration on the four international gateway routers was updated to prevent propagation of excessive routing information.
- The configuration on 144 IP core network routers were updated to change the pre-set limits and default behaviour to not self-isolate in the same situation.

Furthermore, additional key learnings applied were to further strengthen out of band (OOB) and system access with new direct connectivity to the OOB network established from the Optus National Operations Centre; alternate access for 279 routers at 13 exchanges; new passwords on Cisco and IP core routers, with Fortinet and Checkpoint firewalls applied; and a refresh of legacy TACACS user access controls and operational support procedures. The application of these key learnings ensures that in the event of a future network incident, there is timely access to network elements.

Phase 3 was initiated in April 2024 as Optus' strategic network resilience program and includes delivery of on-going resiliency initiatives; residual Phase 2 initiatives; actions and recommendations from technical vendor reviews; and critical lifecycle requirements. Improvements were also made to the welfare check processes in early 2024 and the improved welfare check processes were subject to an independent review, with recommendations from the review implemented. Following this, work commenced to partially automate the welfare check process.

6. Optus' transformation program

The 2022 cyberattack, the 2023 outage and the action taken in October 2024 by the Australian Competition and Consumer Commission (ACCC) against Optus arising from unconscionable conduct and inappropriate sales practices that occurred between August 2019 and July 2023, have clearly highlighted the need for significant transformation across all aspects of Optus' business.

Optus' transformation focuses on the fundamentals – its network, service, security, governance, stakeholder relationships and how the organisation shows up for its customers and Australians.

This means fixing what needs fixing, ensuring clear accountabilities exist within Optus' management structure and strengthening how decisions are made.

With this in mind, the Optus Board appointed Stephen Rue as CEO to oversee a fundamental transformation of the organisation. Mr Rue commenced with Optus in November 2024.

Optus' Transformation Office was established in May 2025 as part of the Chief Operating Officer business unit to coordinate all change efforts across the organization, prioritise activity, track progress, ensure clear accountability and visibility of interdependencies and resolve issues quickly. This work will be critical to ensure Optus delivers on what is required.

Optus acknowledges the need for change and transformation is even more urgent and its transformation plans have continued at an accelerated pace since the Triple Zero outage.

In response to the 2023 outage, Optus implemented a revised strategy which prioritised risk and resilience, as well as simplifying the business to focus on core telecommunications products.

As part of this, capex was prioritised to focus on risk and resilience, and in FY25 approximately half of Optus' $1.4 billion of capital investment was put into risk and resiliency programs across Networks and IT. This investment profile has been carried forward into FY26 and continues to be guiding focus for capex prioritisation.

Relevant to this, the program addresses:

- Strengthening the resilience and reliability of Optus' network – with a Resilience Acceleration Program underway.

- Streamlining complex IT architecture and upgrading critical platforms – prioritising resilience, risk reduction, data enhancements, developing modern architecture, interconnected systems and reducing complexity for customers and employees. This will include simplifying Optus' product set.

- Working urgently to improve processes – process excellence is a key part of Optus' change agenda and Optus is accelerating this work with a rapid expansion of its Process Centre of Excellence team to support process improvement and accountability across the organisation. Approximately 100 processes had already been identified to improve over the next three years with this work now accelerating with additional resources in place.

The challenges Optus faces require discipline and focus. Optus is committed to making the decisions needed to ensure this transformation is successfully executed to achieve sustainable success. This also includes ensuring Optus has the right investment for the pace of change that is required.

Some of the changes that have already been implemented as part of Optus' transformation include:

- Progressive refresh of the Executive Committee to ensure Optus has leaders with the skills and experience to lead through the required transformation. This includes appointments to executive roles overseeing Chief Operating Office, Legal, Security and Risk, Information Technology and Finance.

- Progressive appointments to strengthen leadership capability to support Optus' transformation – including senior appointments for Transformation, Retail, Cyber Security, Compliance, Contact Centres, AI and Data Analytics, Process Excellence, Procurement, Access Network and IP and Transport Network.

- December 2024 – Established a dedicated team to implement change in response to instances of mis-selling, addressing all customer-facing and operational business aspects including customer remediation; mis-selling detection and monitoring; incentives, rewards and consequence management; credit checking and debt collection; vulnerable customer identification; and management and system controls.

- February 2025 – Launched new purpose (*to deliver real choice by championing the customer*) and values (*we are one team; we act with integrity; we are accountable*) to guide Optus' transformation and strategic roadmap.

- May 2025 – Implemented organisational changes to sharpen leadership accountabilities and further strengthen how Optus operates as one team, including establishing the Consumer business unit to increase our focus on our customer service and offering; the Chief Operating Office business unit (including the establishment of the Transformation Office) to support the delivery of Optus' transformation; and announced a new stand-alone business unit to oversee Risk & Compliance at Optus.

- May 2025 – Implemented changes to operating model for Optus' Networks business unit to support the design, build and operation of Optus' network.

- June 2025 – Announced the divestiture of football broadcast rights to Stan Sport to focus efforts on Optus' core business objectives and operations as a telecommunications provider.

- August 2025 – Formally established the Process Centre of Excellence to systematically redesign the way Optus operates to simplify ways of working to benefit customers.

- August 2025 – Announced operating model changes to simplify Optus' delivery model to enable clearer ownership, end-to-end accountability and better outcomes for customers and employees.
- September 2025 – completed development of a long-term 5-year operating plan to guide the strategic development and operational focus of Optus over the coming years.

- Ongoing and frequent improvements across all Optus business units, focusing on reducing complexity, improving customer journeys (including onboarding and purchasing), and internal processes (including supply chain and procurement).

Optus is continuing to work with the telecommunications sector, industry, government and regulators to build on the initiatives already underway as Optus' transformation continues. Further transformation efforts and initiatives that stem from the Independent Review, the ACMA investigation or any other inquiries will be considered carefully and included in future plans for additional activities or changes.

7. Conclusion

The 2025 outage occurred due to an incorrect procedure being followed during a routine and planned upgrade to a firewall at the Regency Park exchange. This error was compounded by failures to escalate the alarms triggered and to respond to customer calls reporting the outage.

Optus is accountable for the failure within its systems and processes and reaffirms its commitment to prioritising the ongoing transformation of the organisation to ensure Optus' network meets the needs and expectations of all Australians – particularly those who rely on Optus to reach emergency assistance.

Optus will continue to work with all levels of government and industry as internal investigations conclude, the findings of the Independent Review and the ACMA investigation are received, in order to ensure its network remains fit-for-purpose. Optus will also continue to collaborate on opportunities to enhance the entire telecommunications ecosystem – including the Triple Zero network.

Optus thanks the Committee for the opportunity to provide this submission with details of the outage, its immediate response and efforts to improve the reliability of Optus systems and services to all Australians.

Appendix A – Timeline of key events leading up to, during and immediately after the 2025 outage based on investigations to date

Date	Time (AEST)	Action	More details
Wednesday 3 September			
03/09/2025		Discussions between Nokia and Optus commenced regarding planning and approval for the upgrade.	
Monday 8 September			
08/09/2025	15:31	Firewall upgrade project team meeting included participants from Nokia and Optus.	Meeting with platform owners to review scope of change for Mobile Core (MC) Interconnect Exchange (IX) Regency Park and a later migration schedule for Rochedale and discuss the impact assessment. Some of the required members of the Optus core network engineering team were not present.
Sunday 14 September			
14/09/2025	07:00	Firewall change request approved by Nokia.	Change approved for deployment for Regency Park IX firewall change (C314593).
Monday 15 September			
15/09/2025	15:48	Nokia confirms the scope of change for E000 trunk blocking and awaiting SBG lock instructions.	Nokia states “As of now, we have been requested to raise change to block the E000 trunks in Regency Park for 18th night work” in the email to Optus indicating the work was to commence on Thursday 18 September in the evening.
Tuesday 16 September			
16/09/2025	08:55	Optus sends an email to Nokia regarding the change process.	The email confirmed that soft locks were required as part of the change.
16/09/2025	21:20	Nokia create the change record for the soft/lock hard lock procedure in Optus' systems.	The risk associated with the change was assessed as 0 / No risk.

Wednesday 17 September			
17/09/2025	11:38	Scheduling of the change emailed ahead of presentation that evening within Nokia.	Change emailed to the emergency change advisory board (eCAB) with approval granted. This was stated to be a low-risk change.
17/09/2025	16:00	Final change presented to emergency change approval board (eCAB) and approved.	Change approval meeting included both Optus and Nokia representation. The purpose of eCAB is to approve the scheduling of the change having regard to other planned changes, not to review it technically.
17/09/2025	17:34	SBG lock change approved in change management system.	Change approved in change management system.
17/09/2025	23:05	Nokia approval of the Method of Procedure (MOP).	Nokia respond to direction to offload creating a change with a MOP to do a soft lock/hard lock "(2 Days Activity - Offload one day and Onload in another day)". Nokia Engineers (Tier 2) approval of change including MOP (C320315). Timestamped by NSM tool.
Thursday 18 September			
18/09/2025	00:00	Firewall upgrade commenced by Nokia.	Implementation of the change process starts 23 hours earlier than originally planned by locking voice serving node (SBG).
18/09/2025	00:17	Soft Lock (also known as graceful shutdown) process starts.	Outage start time.
18/09/2025	00:18	Unsuccessful Triple Zero call – (first).	Networks' system log captures first Triple Zero call attempt which did not connect.
18/09/2025	00:20	Incident ticket raised by Nokia due to spike observed in GDC VoLTE KPIs - IM1918705.	A spike was observed by a Nokia engineer in VoLTE Key Performance Indicator (KPI) performance graphs, used to visualise representations of KPIs for monitoring and assessing the health of VoLTE services. These graphs identified general voice call failures on the bypassed network element. An incident ticket was then raised by Nokia within Optus' systems for attention by Nokia.
18/09/2025	00:47	Incident ticket raised by Optus to Nokia - IM1918762.	Automated emails were generated which contained links to near real-time graphs in Optus' monitoring systems indicating higher call setup failure rates, call drop rates, call registration failure rates and interface call setup failure rates. These graphs highlight general voice call failures on the bypassed network element that were not specifically identified as Triple Zero. These automated emails were reviewed by an Optus engineer. An incident ticket was raised by Optus.

18/09/2025	00:53	Microsoft Teams chat between Optus Senior Networks Engineer and Major Incident Manager – Nokia, escalating awareness of incident.	Optus further contacted Nokia at its command centre (which handles major incidents) through Microsoft Teams highlighting the incident.
18/09/2025	00:56	Microsoft Teams chat between Optus Senior Networks Engineer and Major Incident Manager - Nokia.	Response from Nokia's command centre indicating that the incident was due to the then ongoing change. The incident tickets were then investigated by a Nokia engineer who informed Optus that the activity which caused the alerts was due to ongoing activity related to the change.
18/09/2025	01:12	Incident ticket - IM1918762.	Nokia Engineer adds a description to the IM ticket "Spike observed to failure cause code 503 - Service unavailable due to ongoing activity under PTW-C320315 --> Soft lock / Hard lock and Unlock Mobile SBGs, NBN SBGs and Non-Anchor SBGs in Regency Park to support IP Team firewall activity" and at 1:16:29 this ticket was linked with "C320315".
18/09/2025	01:15	Incident ticket update - IM1918705.	An update is included in the incident ticket stating "failure observing in Volte KPI due to ongoing activity under PTW-C320315 --> Soft lock / Hard lock and unlock mobile SBGs, NBN SBGs and Non-Anchor SBGs in Regency Park to support IP Team firewall activity.
18/09/2025	02:10	Network change completed by Nokia (hard lock) - C320315.	Hard lock component executed on the SBG as per the change activity. All calls expected to have been redirected to alternative node (SBG).
18/09/2025	02:40	Nokia Post- Implementation Change peer review checklist completed	Change peer review check list completed post completion of change. Prior to this, 3 peer reviews completed at 01:52, 09:23 and 13:05 on 17/09/25, none of which identified the issue of the SBG being locked without EPG offload.
18/09/2025	10:13	Offshore Call Centre team receives customer call about Triple Zero issue.	Customer call asks for the details of her local store because her phone wasn't working to call Triple Zero.
18/09/2025	10:47	Offshore Call Centre team receives customer call about Triple Zero issue.	Customer call notifies agent that three or four people with Optus phones are unable to call Triple Zero. The customer confirms person is in hospital and in no immediate danger. Linked to subsequent TIO complaint.
18/09/2025	11:37	Offshore Call Centre team receives customer call about Triple Zero issue.	Customer call tells the agent that four or five people with Optus phones are unable to call Triple Zero. Linked to subsequent TIO complaint.
18/09/2025	12:57	Offshore Call Centre team receives customer call about Triple Zero issue.	Customer call notifies agent that they are unable to make emergency calls using the number Triple Zero although they can make calls to other numbers.

18/09/2025	13:15	Call from SA Ambulance to Optus Operational Architect - EB Delivery regarding possible Triple Zero issue.	SA Ambulance notifies Optus that there is a potential issue with emergency calls. Asks the Optus contact if there is an issue with Triple Zero of which the contact says they are not aware of any. SA Ambulance contact says they will confirm. Call duration 37 seconds.
18/09/2025	13:17	Call from SA Ambulance to Optus Operational Architect - EB Delivery confirming Triple Zero issue.	SA Ambulance confirms with Optus Operational Architect – EB Delivery that there are issues with emergency calls. Optus confirms they will escalate internally. Call duration 25 seconds.
18/09/2025	13:25	Call from SA Ambulance to Optus Operational Architect - EB Delivery asking for update.	SA Ambulance calls Optus requesting an update on the emergency call issue identified. Optus confirms the issue is being escalated. Call duration 15 seconds.
18/09/2025	13:26	Call from Optus Operational Architect - EB Delivery to Optus Incident Manager - EB Delivery Major Incident Management (MIM) advising of Triple Zero issue.	Optus Operational Architect – EB Delivery advised the Optus Incident Manager - EB Delivery Major Incident Management (MIM) that a contact from SA Ambulance has alerted them to a Triple Zero issue from Optus mobile phones in SA. Call duration 1 minute and 56 seconds.
18/09/2025	13:31	Optus State Radio Provisioning & Quality team commences internal testing to Triple Zero.	Optus State Radio Provisioning & Quality team commence test calls to Triple Zero.
18/09/2025	13:32	Optus Operational Architect - EB Delivery internal Incident ticket raised for investigation.	Optus Operational Architect - EB Delivery raises an internal ticket in Service Now for investigation, case OBCS6994116 with a short description of "Mobile - Optus mobile users in South Australia have reported they are unable to call Triple Zero". Further details set are "Impact: 1 - Enterprise", "Urgency: 1 - Critical" and "Priority: 1 - Critical".
18/09/2025	13:38	Networks Major Incident Management, Nokia and Optus, meeting via MS Teams.	Networks Major Incident Management technical call established with Nokia Operations, Nokia Tier 2 support, Optus Engineering, Optus South Australia field team, Optus Operations. Technical investigation commences. Nokia Optus Command Centre (OCC) team initiated this call in Teams. Bridge opened and remained open until complete.
18/09/2025	13:51	Major Incident Declared.	Optus Incident Manager – EB Delivery declares Major Incident (HPIM #OBCS6994150)" with the description "Mobile - Optus mobile users in South Australia have reported they are unable to call Triple Zero. 1 - Critical ... OBCS6994150 .... The Optus Network Management Centre has been engaged to investigate; we will provide the next update by 14:50."
18/09/2025	13:53	South Australia police report issue with Triple Zero failure calls to Optus Emergency Services Support (ESS) team, operated in Australia on Optus' premises by Nokia.	SA police call into ESS to report unsuccessful Triple Zero calls.

18/09/2025	14:09	Microsoft Teams message from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety.	Optus Director - Network & Service Operations requests an urgent call from Optus Director - Security & Public Safety regarding issue with Triple Zero calls in SA/WA.
18/09/2025	14:10	Optus MIM (Major Incident Management) team hold a Networks Technical Investigation Bridge.	Optus MIM Team advised on the incident call the outage was potentially caused by the Regency Park firewall change. “…potential correlation to the Change (C320315_for blocking SBGs in Regency Park)”.
18/09/2025	14:11	Offshore Call Centre team receives customer call about Triple Zero.	Customer tells agent they tried to make an emergency call and could not do so from two Optus mobiles. Customer had to get a neighbour, and the call went through on their phone.
18/09/2025	14:11	Call from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety.	Call from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety for an update on the issue with Triple Zero calls. Call duration was 3 minutes and 25 seconds.
18/09/2025	14:16	Text messages from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer.	Text message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer stating that there is a network issue identified impacting calls to “Triple Zero in SA & WA since 3am. Network change caused it, now being rolled back” In subsequent text messages the Chief Corporate Affairs & Marketing Officer asks "Did we only get told about this? How many calls?" and Optus Director - Security & Public Safety answers "...Found out about 30 minutes ago ... unsure of volume of calls yet ... Current advice is 10 failed calls to TZ today."
18/09/2025	14:19	Text message from Optus to Telstra Emergency Call Person (ECP).	The message stated that an issue had been identified with Triple Zero call from SA and WA, which Optus was investigating.
18/09/2025	14:20	Optus Network Engineering requests rollback on incident call.	Optus Engineering instructed Nokia verbally to unlock the SBGs in Regency Park. This was noted in the chat at 14:25 "Action ongoing: We are unlocking o5RXVasSBG".
18/09/2025	14:23	Roll back commenced.	Roll back in progress. The first unlock command was issued at 14:23:32.
18/09/2025	14:24	Email from Optus Director - Security & Public Safety to Optus VP - Corporate Communications and Optus Associate Director - Government Affairs.	Email from Optus Director - Security & Public Safety advising of an issue identified by networks team impacting calls to Triple Zero in SA and WA. This triggers team to begin arranging notification process.

18/09/2025	14:29	Commencement of data collection process to support Welfare Check.	Optus Duty Director verbally asks Nokia to supply Call Detail Records (CDR) to Optus relating to the unsuccessful Triple Zero calls by consolidating impacted services into a list of customers to be contacted.
18/09/2025	14:29	Microsoft Teams from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety.	Optus Director - Network & Service Operations messages Optus Director - Security & Public Safety stating, "64 attempts yesterday, today attempts 10 for WA & SA". This refers to a comparison of the previous day's Triple Zero call attempts between 12:00-13:00 and this day to aid with incident investigation.
18/09/2025	14:31	Optus Associate Director - Government Affairs calls Senior Adviser - Minister for Communications.	Call was not answered, and no message was left.
18/09/2025	14:31	Last unsuccessful Triple Zero call.	Networks log of the last unsuccessful Triple Zero call related to the incident.
18/09/2025	14:31	Unlocking of the SBG complete.	The node impacting Triple Zero began unlocking at 14:29 and finished unlocking at 14:31. The unlocking restored normal service.
18/09/2025	14:33	Microsoft Teams from Optus Director - Security & Public Safety to Optus Director - Network & Service Operations.	Optus Director - Security & Public Safety message to Optus Director - Network & Service Operations indicated they have checked the Triple Zero disruption protocol for any steps required. Optus Director - Network & Service Operation asked to receive confirmation of authorities that have been contacted.
18/09/2025	14:34	Outage resolution time.	The issue was tested and confirmed to be resolved. Optus staff in SA and WA confirm Triple Zero call success.
18/09/2025	14:34	Call from Senior Adviser - Minister for Communications to Optus Associate Director - Government Affairs.	Senior Adviser to Minister for Communications calls Associate Director, Government Affairs and is informed of the issue with Triple Zero calls in WA and SA and that Optus would send through an email when resolved. Call duration was two minutes.
18/09/2025	14:35	Email sent internally to business and networks stakeholders regarding Networks Major Incident.	Internal Pager Duty notification sent regarding a Networks Major Incident titles Optus users in SA, WA & NT have reported they are unable to call 000.
18/09/2025	14:37	Email from Optus Emergency Services Support (ESS) team to SA Police & WA Police.	ESS team email to WA and SA Police advising that Triple Zero outage had been resolved for SA and waiting on testing for WA.
18/09/2025	14:42	Call from Optus Director - Security & Public Safety to ACMA Manager National Interests.	Optus Director - Security & Public Safety calls ACMA Manager National Interests to inform them of an issue with Triple Zero calls in WA and SA and that Optus would send through an email when resolved.

18/09/2025	14:43	Microsoft Teams from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety.	Optus Director - Network & Service Operations confirms that the rollback appears to have been done around 14.30. The Optus Director - Security & Public Safety asks if Triple Zero calls are working again. Optus Director - Network & Service Operations confirms they are.
18/09/2025	14:45	Email from Optus Associate Director - Government Affairs to Senior Adviser - Minister for Communications.	Optus email sent to cialerts@communications.gov.au Copied: xxxx@mo.communications.gov.au>; Optus Government Affairs MPsupport@optus.com.au Email provides notification that "… Optus has received reports that some customers in SA and WA are experiencing impacts to Triple Zero calls. Suspected cause has been indicated to stem from our Regency Park exchange ... have commenced the welfare check processes and relevant protocols.".
18/09/2025	14:47	Optus Chief Corporate Affairs & Marketing Officer and Optus CTO call Optus Director - Security & Public Safety.	Optus Director of Security and Public Safety provides a briefing on the Triple Zero outage
18/09/2025	14:50	Call from Optus Director - Security & Public Safety to SA Police Chief Inspector.	Advising details of the Triple Zero outage.
18/09/2025	14:51	Optus Executive Committee (including Optus CEO) verbally notified of Triple Zero outage.	Optus CTO and Chief Corporate Affairs & Marketing Officer notify the Executive Committee including the Optus CEO of the Triple Zero issue.
18/09/2025	14:52	Email from Optus Associate Director - Government Affairs to Senior Adviser - Minister for Communications.	Optus email sent to cialerts@communications.gov.au Copied: xxxx@mo.communications.gov.au>; Optus Government Affairs MPsupport@optus.com.au Providing notification that "… services have returned to normal … protocol reporting shows that 10 calls may have been impacted ... and welfare checks will be made."
18/09/2025	14:54	Text message from Optus Associate Director - Government Affairs to Senior Adviser - Minister for Communications.	Confirming 'services have returned to normal'.
18/09/2025	14:55	Microsoft Teams from Optus Director - Network & Service Operations to Optus Director - Security & Public Safety.	Optus Director - Security & Public Safety asking "… is it only fixed line calls that go through the SBGs? Is that why the numbers were low? SA Police just called me. They were happy to hear the volumes are low " and "Govt Affairs notified Dept of Comms and Minister's Office ...".

18/09/2025	14:58	Text message from Optus Director - Security & Public Safety to Telstra Emergency Call Person (ECP).	Optus Director of Security and Public Safety advised issue is now resolved by rolling back a network change. Advised only 10 Triple Zero calls impacted and that Optus had notified ACMA, SA Police, WA Police, Department of Communications (DITRDCSA) and Minister's Office.
18/09/2025	15:04	Microsoft Teams from Optus Director – Network & Service Operations to Optus Director – Security & Public Safety. Optus Director Network & Service Operations and Optus Security & Public Safety.	Optus Director - Network & Service Operations requests a call with Optus Director – Security & Public Safety following from their Microsoft Teams conversation at 14:55 on 18 September 2025.
18/09/2025	15:15	Text message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer.	Text message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer advising "Significant Network Outage notifications about to be sent, as required by the regulations.".
18/09/2025	15:17	ACMA SNO (Significant Network Outage) notification sent.	Notification sent. In addition to Optus internal stakeholders, addressees included ACMA, Telstra and Concentrix ECP.
18/09/2025	15:18	Call from Optus Principal Incident Manager, Optus Networks Operations to Telstra Emergency Support team.	Call to ensure the SNO notification had been received.
18/09/2025	15:26	SNO notification re-sent including correct Telstra address.	There was an error in the email address used for Telstra in the 15:17 email notification. This notification corrected the error.
18/09/2025	15:27	ACMA SNO (Significant Network Outage) notification sent.	Correction email to SNO notification sent at 3:17pm to: Optus internal stakeholders, ACMA, Telstra ECP and Concentrix ECP. Correction was to the date of the outage which was originally advised to be 19/09/2025 and was corrected to the 18/09/2025.
18/09/2025	15:48	Nokia provided unsuccessful CDR data related to Triple Zero calls to Optus Duty Director.	Nokia provided Optus with the CDRs which showed no unsuccessful calls. The technical nature of the fault meant that unsuccessful Triple Zero calls were not captured in the data as the calls did not reach the part of the core network from which the records are usually obtained.
18/09/2025	16:05	Optus engineering team review data collection processes.	Optus engineering team develop a new method to identify and extract unsuccessful Triple Zero calls. This process was both complex and time-intensive, involving multiple iterations and refinements to accurately identify the affected customers.

18/09/2025	16:47	Text Message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer.	Optus Director - Security & Public Safety sends a text message to Optus Chief Corporate Affairs & Marketing Officer with an update stating, "volumes of failed calls unknown ... Networks now checking the probes data, but that may take several hours".
18/09/2025	17:30	Optus Chief Technology Officer update to Optus Executive Committee.	Update from CTO to Optus Executive Committee regarding the Triple Zero outage.
18/09/2025	17:51	Phone call from Optus Director - Security & Public Safety to Head of Telstra ECP.	Optus Director - Security & Public Safety calls the Head of Telstra ECP to provide an update on situation.
18/09/2025	18:00	Optus Network Incident Response Team (NIRT) Meeting.	Optus Chief Technology Officer (and other ExCo) receive an update on the progress of the search for failed Triple Zero call data collection process.
18/09/2025	18:30	Optus Networks team proceed with sourcing an alternative method to capture impacted Triple Zero Calls.	Optus Networks team deep-dive call capture commenced. There was not an known process for identifying calls and it was necessary to scan multiple systems to identify the necessary data.
18/09/2025	19:05	Optus Networks convene to discuss their analysis and potential solutions.	Optus Engineering requested all teams working on sourcing the data to discuss and align the approach.
18/09/2025	19:50	Optus engineering teams captures data for first tranche of 100 impacted Triple Zero calls.	100 impacted customers identified through the analysis of data extracted from systems.
18/09/2025	20:05	Text message exchange from Director - Security & Public Safety to Chief Corporate Affairs & Marketing Officer.	Director - Security and Public Safety sends an text message to Chief Corporate Affairs & Marketing Officer advising data for 100 impacted Triple Zero customers captured and waiting for an update on whether Welfare Checks would occur that night.
18/09/2025	20:08	Text Message from Optus Director - Security & Public Safety to Optus VP - Corporate Communications.	Update on the volume of impacted calls (100) as well as next steps and process for Welfare Checks and timing of completion, reporting obligations.
18/09/2025	20:08	Welfare Check list provided by Optus Networks to Contact Centre Team.	Optus Principal - Major Incident Management provides 100 impacted services (unsuccessful Triple Zero) covering the period 18/09/2025 00:40 AEST to 14:34 AEST. Includes phone number, cell tower, state. No customer name / details.

18/09/2025	20:15	Text Message from Optus Director - Security & Public Safety to Chief Inspector - SA Police.	Optus Director - Security & Public Safety sends a text message to Chief Inspector - SA police with an update. Volume across SA, WA, NT was 100. Optus also confirms 50 of the calls relate to SA customers.
18/09/2025	20:30	Meeting held with Optus VP - Operations, Optus Chief Technology Officer, Optus VP - Core Network, Optus Senior Director - Mobile Core & Service Eng, Optus Director - Network & Service Operations.	Follow up between Optus NIRT and Optus Chief Technology Officer regarding the search progress on the 100 failed Triple Zero calls and search criteria.
18/09/2025	20:34	First cycle of Welfare Check process commenced by Optus Contact Centre team.	First call at 20:34 by Contact Centre team.
18/09/2025	20:43	Fatality advised of by customer to Optus Contact Centre during Welfare Check call.	Optus advised through Welfare Check of first fatality where no confirmation Emergency Services were reached.
18/09/2025	21:01	Fatality advised of by customer to Optus Contact Centre during Welfare Check call.	Optus advised through Welfare Check of fatality where no confirmation Emergency Services were reached.
18/09/2025	21:33	First tranche of Welfare Check calls completed.	Last Welfare Check call began at 21:29.
18/09/2025	21:33	Data prepared by Optus Contact Centre team for police Welfare Checks.	Gathering customer data from Optus and partner data team to notify police for referrals. Data process concluded at 22:43.
18/09/2025	22:57	Police referrals – NSW.	Contact Centre sent Police referrals via email to NSW Police.
18/09/2025	23:00	Police referrals – VIC.	Contact Centre sent Police referrals via email to VIC Police.
18/09/2025	23:02	Police referrals – SA.	Contact Centre sent Police referrals via email to SA Police.
18/09/2025	23:04	Police referrals – WA.	Contact Centre sent Police referrals via email to WA Police.
18/09/2025	23:06	Optus Contact Centre leader notified of fatalities.	Optus Community Manager - Contact Centre debriefed with team and learned about two fatalities.

18/09/2025	23:28	Email update confirming Welfare Check completion from the Customer Centre Team to CTRE Escalations, cc Duty Directors, OB Network SD, SMB Compliance, Wholesale Service Desk.	Email confirmation of Welfare Check completion. Fatalities not identified in this email. The email covers volume of calls referred to police.
18/09/2025	23:38	Optus Networks Engineering team acquire additional data.	Optus Networks Engineering team finalise list of impacted emergency calls during the period (00:30-15:00) after refining method of data capture. Optus Engineering team had analysed bearer setup between the handset and the Packet Gateway – resulting in a further 524 customers affected, total 624.
18/09/2025	23:39	Internal email update from the Optus Networks team.	Advising 624 Optus customers affected, including a breakdown of customers per state.
Friday 19 September			
19/09/2025	00:25	Email from Optus Community Manager – Contact Centre to Optus VP - Customer Contact Centres, Optus VP - Operations and Optus Director - Security & Public Safety notifying of fatalities.	Optus Community Manager - Contact Centre provides summary update of Welfare Checks including a reference to potential loss of lives.
19/09/2025	06:00	Meeting with Optus VP - Operations, Optus Senior Director - Technical Network Assurance, Optus Director - Networks & Service Operations, Optus Principal - Major Incident Management.	Optus networks team meeting to discuss and validate data from previous evening (524 additional impacted customers). It was determined at this meeting that further validation of the data was required. They discuss escalating to senior executives including Optus Chief Technology Officer, Optus Chief Corporate Affairs & Marketing Officer and Optus VP - Customer Contact Centres.
19/09/2025	06:21	Text message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer.	Advising of potential loss of lives, noting information being clarified.
19/09/2025	06:26	Email from Optus Director - Security & Public Safety to Optus VP - Customer Contact Centres, Optus VP -Operations, Optus Community Manager.	Request for more information relating to '3 extreme cases' in case external stakeholders including the minister require notification.
19/09/2025	06:34	Email confirmation from Optus contact centre team to Optus Community Manager - Welfare Check calls completed.	A more detailed email summary of Welfare Check calls from the previous day provided including information on fatalities.
19/09/2025	06:57	Text message from Optus Director - Security & Public Safety to Optus Chief Corporate Affairs & Marketing Officer.	Confirms customers referred to a fatality during Welfare Check calls. In addition the message notes a meeting will be held at 07:30 to find out more (meeting moves to 7:45).

19/09/2025	07:33	Chief Corporate Affairs & Marketing Officer calls Director – Security and Public Safety.	Verifying details of the outage, failed calls, and outcomes of Welfare Checks and preparing to escalate it. Duration two mins.
19/09/2025	07:37	Call from Optus Chief Corporate Affairs & Marketing Officer to CEO.	Unanswered.
19/09/2025	07:45	Senior Stakeholder meeting held.	Regroup with key executives to discuss next steps. Attendees included Optus Senior Director - Technical Network Assurance, CTO, Optus VP - Operations and Optus Director - Network & Service Operations.
19/09/2025	08:13	Call from CEO to Optus Chief Corporate Affairs & Marketing Officer.	Returned call in which Optus Chief Corporate Affairs & Marketing Officer informs CEO of the fatalities learned of overnight.
19/09/2025	08:45	Call from Optus VP - Contact Centres, AI & Analytics to Optus Chief Operating Officer to inform of fatalities.	Phone call from Optus VP - Contact Centres, AI & Analytics. Optus Chief Operating Officer subsequently spoke to Optus Chief Corporate Affairs & Marketing Officer shortly after and then met with Optus VP – Contact Centres, AI & Analytics again at approximately 10am.
19/09/2025	08:52	Call from Optus CEO to Optus Board Director and Singtel Group CEO, Yuen Kuan Moon.	Advising key facts as they were understood at the time. Call to Mr Yuen as Mr Arthur was on leave overseas at the time.
19/09/2025	09:00	Crisis Management Team (CMT) initial meeting (Teams and in person).	Attendees: CMT Coordinator alongside representatives from Corporate Communications, Networks, Consumer, Customer Contact Centre, Government Relations, Networks Regulatory, People & Culture. Meeting held to discuss current situation and actions for each key team. CEO is dialed into the CMT at 09:10.
19/09/2025	09:10	Text message from Optus CEO to Optus Chairman.	Update provided relating to key facts as they were understood at the time including Triple Zero outage and fatalities. Initially call (unanswered) then follow up text message to Optus Chairman, John Arthur, as Mr Arthur was on leave overseas at the time.
19/09/2025	10:00	First Optus Incident Crisis Communications Team (ICCT) Meeting.	Attendees included: Representatives responsible for corporate communications, government relations, customer communications, employee communications and ICCT coordination. Meeting held to provide update on current situation, assign roles and actions for each key team.
19/09/2025	10:00	Additional Welfare Check list (524) provided by Optus Networks to Contact Centre team.	Optus Principal - Major Incident Management provides list of additional 524 impacted services (failed Triple Zero) and preparatory work for Welfare Check calls begins.

19/09/2025	10:00	Email invitation sent to Optus Executive for first CMEC meeting.	Email invites noted meeting being held at 11am. Invitees included: Optus Executive Committee with CEO Chief of Staff, CMEC/CMT Coordinator and Organisational Resilience support
19/09/2025	10:09	Update to CMT using MS Teams chat.	Optus VP - Operations messages the CMT Microsoft Teams Chat (named "CMT Activation: Failed Triple Zero Calls) with the update that the file of 524 calls has been provided to the customer centre team.
19/09/2025	10:16	Email from Chief Inspector - SA Police to Optus Director - Security & Public Safety.	Regarding first tranche of Welfare Check calls, SA Police advise Welfare Checks not required as they believed they had been conducted by Optus. Optus responds with confirmation that Welfare Checks were required to be conducted by police and detail resupplied.
19/09/2025	10:28	Text message from Optus CEO to non-executive director of the Optus Board.	Text message sent by the Optus CEO to Michaela Browning advising key facts as they were understood at the time.
19/09/2025	10:30	Text message from Optus CEO to non-executive director of the Optus Board.	Test message sent by the Optus CEO to Nicki Tan advising key facts as they were understood at the time.
19/09/2025	10:30	Action to set up resources for second set of Welfare Checks.	Optus Community Manager – Global Contact Centre and two members of the Optus Customer Centre Team, prepare training and scripting for team.
19/09/2025	10:33	Text message from Optus CEO to non-executive director of the Optus Board.	Text message sent by the Optus CEO to Andrew Parker advising of key facts as they were understood at the time.
19/09/2025	10:42	Email from WA Police A/Manager - Telephony Services to Optus Director - Security & Public Safety.	WA Police requesting additional information relating to the services referred for Welfare Checks. Optus Director - Security & Public Safety provided additional details at 18:16.
19/09/2025	10:49	Email from Optus Director - Security & Public Safety to WA Police A/Manager - Telephony Services	Optus Director - Security & Public Safety acknowledged the WA Police A/Manager's email of 10:42 and indicated that Optus would revert with more details.
19/09/2025	10:54	Call from Optus VP - Corporate Communications to Optus VP – Singtel Group Corporate Affairs & IR, Group Corporate Affairs and Investor Relations.	Call to provide a briefing on current situation.
19/09/2025	11:00	Crisis Management Executive Committee (CMEC) Meeting.	Attendees included: Optus Executive Committee with CEO Chief of Staff, CMEC/CMT Coordinator and Organisational Resilience support

			Apologies: Chief Customer Officer – Enterprise and Business
19/09/2025	11:00	Set up contact centre staff for second tranche of Welfare Checks.	Contact centre team conducting Welfare Checks complete training re: documentation, scripting and Welfare Check process.
19/09/2025	12:00	Second Optus Incident Crisis Communications Team (ICCT) Meeting.	Attendees included: Representatives responsible for corporate communications, government relations, customer communications, employee communications and ICCT coordination.
19/09/2025	12:04	Second tranche Welfare Check calls commenced.	Additional 524 Welfare Check calls commence.
19/09/2025	12:17	Email from Optus Director - Security & Public Safety to A/Manager - Telephony Services - WA Police.	Requested contact details for commissioner or police minister. Response advising they cannot pass the details on to Optus, will escalate to their Superintendent.
19/09/2025	12:40	Fatality advised of by customer to Optus Contact Centre during Welfare Check call.	Optus advised through Welfare Check of fatality where no confirmation Emergency Services were reached.
19/09/2025	13:00	Second CMT Meeting.	Attendees: CMT Coordinator alongside representatives from Corporate Communications, Networks, Consumer, Customer Contact Centre, Government Relations, Networks Regulatory, People & Culture. Agreed for CEO to hold press conference at 15:10. Noted board meeting occurring at 15:00. Employees to be notified prior to media announcement.
19/09/2025	14:00	Second CMEC Meeting.	Attendees include: Optus Executive Committee with CEO Chief of Staff, CMEC/CMT Coordinator and Organisational Resilience support 1. Update on key discussions from CMT. 2. Update on media conference and contact required with relevant government/regulatory bodies and employees. 3. Update on board meeting.
19/09/2025	14:00	The second tranche of Welfare Check calls completed.	Optus Customer Centre Team emails the Optus Community Manager confirming all Welfare Checks complete.
19/09/2025	14:08	Email from Optus Chief Corporate Affairs & Marketing Officer to Optus Board.	Email with draft talking points provided.

19/09/2025	14:18	Optus VP Corporate Communications emails Singtel Corporate Affairs team.	Advises the plan is to speak to media at 15:30 and that regulators and government contacts will be briefed prior to media conference. Also, confirms CEO has spoken to Group Chief Executive Officer.
19/09/2025	14:33	Email exchange Optus Directors and Optus CEO	Notifying details then understood of the Triple Zero outage in SA, WA and NT.
19/09/2025	14:36	Optus CEO calls ACMA Chair.	CEO advises ACMA Chair of the network issue resulting in unsuccessful Triple Zero calls as well as known fatalities Optus became aware of during Welfare Checks.
19/09/2025	15:00	Optus Board meeting.	Board meeting ran from 15:00 to 15:35 with a focus on Triple Zero outage. The Board was provided an update on the Triple Zero outage impacting SA, WA, NT and known fatalities, as well as the plan to inform key stakeholders and plan to hold a media conference that afternoon.
19/09/2025	15:15	Email from SA Police to Director, Security & Public Safety.	Regarding Welfare Check process.
19/09/2025	15:45	Third Optus Incident Crisis Communications Team (ICCT) Meeting.	Attendees included: Representatives responsible for corporate communications, government relations, customer communications, employee communications and ICCT coordination.
19/09/2025	15:49	Call from to Acting Deputy Secretary - Department of Communications (DITRDCSA) to Optus Chief Corporate Affairs & Marketing Officer.	Incoming call was missed.
19/09/2025	15:54	Call from Senior Adviser - Minister for Communications to Optus Associate Director - Government Affairs.	Call duration two minutes.
19/09/2025	16:03	Call from Optus Chief Corporate Affairs & Marketing Officer to Acting Deputy Secretary - Department of Communications (DITRDCSA).	Optus provided an update on Triple Zero outage, fatalities and intended press conference.
19/09/2025	16:09	Email from Optus Chief Corporate Affairs & Marketing Officer to Board.	Provided draft talking points.
19/09/2025	16:12	Call from Optus Chief Corporate Affairs & Marketing Officer to Chief of Staff - Communications Minister.	Not answered.

19/09/2025	16:14	Call from Optus Chief Corporate Affairs & Marketing Officer to Acting Secretary for the Department of Communications.	Not answered.
19/09/2025	16:17	Call from Optus Chief Corporate Affairs & Marketing Officer to Acting Secretary for the Department of Communications.	Missed call.
19/09/2025	16:22	Call from Optus Chief Corporate Affairs & Marketing Officer to Acting Secretary - Department of Communications (DITRDCSA).	Returning an earlier call (16:17) – left a message.
19/09/2025	16:23	Call from Chief of Staff - Communications Minister to Optus Chief Corporate Affairs & Marketing Officer.	Duration 9 minutes.
19/09/2025	16:26	Network emergency embargo.	A temporary change embargo is put in place by networks, preventing other changes being made to the network.
19/09/2025	16:33	Call from Optus Chief Corporate Affairs & Marketing Officer to Acting Secretary Department of Communications (DITRDCSA).	Call duration was 8 minutes.
19/09/2025	16:36	Email to media.	Optus sends media invitation to press conference.
19/09/2025	16:41	Police referrals – additional Welfare Checks SA.	Contact Centre sent police referrals via email to SA Police.
19/09/2025	16:41	Police referrals - additional Welfare Checks NSW.	Contact Centre sent police referrals via email to NSW Police.
19/09/2025	16:43	Police referrals - additional Welfare Checks QLD.	Contact Centre sent police referrals via email to QLD Police.
19/09/2025	16:45	Police referrals - additional Welfare Checks NT.	Contact Centre sent police referrals via email to NT Police.
19/09/2025	16:47	Police referrals - additional Welfare Checks WA.	Contact Centre sent police referrals via email to WA Police.
19/09/2025	16:48	Police referrals - additional Welfare Checks TAS.	Contact Centre sent police referrals via email to TAS Police.
19/09/2025	16:54	Call from Chief of Staff to Communications Minister to Chief Corp Affairs & Marketing Officer.	Call duration was two minutes.

19/09/2025	17:08	Call from Chief Inspector - SA Police to Optus Director - Security & Public Safety.	Missed call.
19/09/2025	17:12	Call from Optus Director - Security & Public Safety to Chief Inspector - SA Police.	Returns call and provides an update on the situation.
19/09/2025	17:18	Call from Optus Director - Security & Public Safety to A/Manager - Telephony Services WA Police.	Seeking contact points to brief on press conference.
19/09/2025	17:20	Optus VP – Corporate Communications emails Singtel Corporate Affairs.	Provided with talking points planned for press conference that afternoon.
19/09/2025	17:45	Optus media conference held.	Optus CEO holds media conference.
19/09/2025	17:51	Call from Optus Director - Security & Public Safety to –Telstra ECP.	Advised of Optus CEO press conference.
19/09/2025	17:52	Call from Optus Head of Regulatory & Government Affairs to Chief of Staff – WA Premier.	Call went to voicemail.
19/09/2025	17:52	Call from Optus Senior Director - Local Community Engagement to Chief of Staff - SA Premier.	Call went to voicemail.
19/09/2025	17:54	Text message from Optus Senior Director - Local Community Engagement to Chief of Staff - SA Premier.	Text message requesting call back.
19/09/2025	17:54	Text message from Head of Regulatory and Government Affairs to WA Premier - Chief of Staff.	Text message requesting call back.
19/09/2025	17:54	Call from Optus Director, Security & Public Safety to Chief Inspector – SA Police.	Advise details of press conference being held by Optus CEO. Police requested information.
19/09/2025	17:55	Call from Optus Head of Regulatory & Government Affairs to Chief of Staff - Emergency Services Minister WA.	Not answered, sent text message.

19/09/2025	17:57	Call from Optus Head of Regulatory & Government Affairs to Chief of Staff - NT Chief Minister.	Call went to voicemail.
19/09/2025	17:57	Text message from Optus Head of Regulatory & Government Affairs to Chief of Staff - NT Chief Minister.	Text message sent requesting call back.
19/09/2025	17:58	Email from Senior Adviser - Prime Minister's Office to Optus Head of Regulatory & Government Affairs.	Optus Head of Regulatory & Govt Affairs receives an email from Senior Adviser - Prime Minister's Office requesting "… all relevant information on yesterday's outage, which the Department has just informed me about.".
19/09/2025	17:58	Call from Optus Associate Director - Government Affairs to Senior Adviser - Shadow Communications Minister's Office.	Provided update on talking points and situation as it stood - advised would be in contact over weekend.
19/09/2025	18:00	Third CMEC Meeting.	Attendees include: Optus Executive Committee with CEO Chief of Staff, CMEC/CMT Coordinator and Organisational Resilience support.
19/09/2025	18:00 – 21:26	Optus continues communications with government, emergency services and industry stakeholders.	
19/09/2025	18:48	Singtel Stock Exchange Announcement.	SGX statement filed.
19/09/2025	18:48	Optus statement.	Statement from media conference published on Optus website.
19/09/2025	20:19	SA Premier calls Optus CEO.	SA Premier returns call to Optus CEO to discuss the situation and request further information on fatalities.
Saturday 20 September – Wednesday 24 September (key external communications and board meetings)			
20/09/2025	11:23	Optus CEO calls Minister for Communications.	CEO provides an update on the current situation and plan for press conference.
20/09/2025	15:20	Media conference.	CEO held Media conference at 15:20.
20/09/2025	16:06	Email sent from WA Police to Optus Director, Security & Public Safety.	Formally advising Optus of a second fatality in WA where no emergency services were reached which appeared to have occurred during the outage period.

20/09/2025	16:34	Optus CEO calls WA Premier.	Advised second fatality in WA.
20/09/2025	17:43	Optus statement published.	Statement from media conference published on Optus website.
20/09/2025	17:44	Optus statement regarding fourth fatality.	Optus publishes statement regarding fourth fatality related to Triple Zero failures on Optus website.
20/09/2025	21:30	Optus Board meeting.	Board meeting ran 21:30 – 23:20. The focus of the meeting was for management to provide the Board with an update, including key events and stakeholder engagement and to establish a Response Oversight Committee to recommend to the Board a third party conduct an independent review including its terms of reference.
21/09/2025	~12:00	Optus commences additional reviews of data to check the numbers of impacted service numbers.	This process led to the identification of seven further impacted customers.
21/09/2025	15:15	Media conference.	CEO held media conference.
21/09/2025	19:00	Optus Board meeting.	Board meeting ran 19:00 – 20:15. The focus of the meeting included an ongoing update of the events and stakeholder engagement, additional controls implemented by networks and other actions being taken by management. CEO provided an update on his plan to keep the media and public updated.
22/09/2025	12:20	A third tranche of impacted customers was identified, comprising seven impacted customers.	These service numbers were impacted in the period between the commencement of the outage and 00:30 AEST on 18 September 2025, which was not within the original search parameters based on Optus' then understanding of the time period of the outage.
22/09/2025	13:58	Further Welfare Check calls commence.	
22/09/2025	14:14	Further Welfare Check calls conclude.	
22/09/2025	14:23	Data relating to unsuccessful Welfare Checks provided to police.	
22/09/2025	~ 15:45	Optus statement regarding additional seven customers impacted.	Statement regarding an additional seven customers impacted by Triple Zero failures during the outage period. Statement noted on 18 September the time between 00:17 – 00:30 had not previously been accounted for provided to stakeholders and media. Note: This resulted in

			a total of 631 customers estimated as impacted over the period from 00:17 to 15:00 on 18 September 2025.
22/09/2025	20:00	Optus Board – Response Oversight Committee meeting.	The meeting ran from 20:00 – 21:30. The focus of the meeting included management providing the Board with an update on key events and stakeholder engagement.
23/09/2025	16:00	Optus Board meeting.	The meeting ran from 16:00 – 18:00. The focus of the meeting included management providing the Board with an update on key events and stakeholder engagement. During this meeting the Board approved the appointment of the Independent Reviewer and proposed terms of reference.
24/09/2025	14:00	Media conference.	CEO held media conference at 14:00.
24/09/2025	18:00	Optus Board – Response Oversight Committee meeting.	The meeting ran from 18:00 – 18:58. The focus of the meeting included management providing the Board with an update on key events and stakeholder engagement, and discuss ongoing actions work within network operations.

Appendix B – Glossary of terms

ACCAN	Australian Communications Consumer Action Network	**MOP**	Method of Procedure
ACMA	Australian Communications and Media Authority	**Nio metrics**	Data probe
AMTA	Australian Mobile Telecommunications Association	**NSET**	Network service experience team
ATA	Australian Telecommunications Alliance	**NSM**	Network Service Manager
Camp -On	access an alternate network in a failover scenario	**OCC**	Optus Command Centre
CDR	Call Detail Record	**Operational Architect, EB Delivery**	Technical expert aligned with customer in Enterprise & Business Delivery
CMT	Crisis Management Team Optus	**Pager Duty**	Optus internal notification SMS & Email
CMEC	Crisis Management Executive Committee	**Project Team**	Firewall upgrade project team
Customer Contact Time	For the purpose of this timeline, we have recorded the time which the customer talked to the agent	**RAN**	Radio Access Network
EAP	Employee Assistance Project	**SBG**	Session Border Gateway physical device
EB Delivery	Enterprise & Business Delivery	**Scrub**	scraping logs from to identify usable data
ECP	Telstra Emergency Call Person	**ServiceNow**	ServiceNow event ticketing tool used by Optus
ESS	Emergency Sensitive Support	**SIP**	Session initiation Protocol
Grafana	Data monitoring tool	**SLT**	Senior leadership Team
Hard Embargo	stop on all change activity, Change Freeze	**SMS**	Short message Service
HPIM	High Priority Incident Management	**SNO**	Significant Network Outage
HyperCare	Highest level of support and focus with Nokia above a priority 1 (immediate and full attention)	**SRPQ**	State Radio and Provisioning and Quality
ICCT	Incident crisis communications team	**TIO**	Telecommunications Industry Ombudsman
IVR	Interactive Voice Response		
MIM	Major Incident Manager		