Independent Report

The Triple Zero Outage at Optus: 18 September 2025

Prepared for the Board of Optus by Kerry Schott AO

12 December 2025

Acknowledgements

To Country – I acknowledge the Traditional Custodians of the land on which I work and live and on which Optus operates. Respect is paid to Elders past and present and their continued connection to country.

For Assistance – I acknowledge the support and assistance provided by the Boards of Optus and Singtel and by the Executives and other employees of Optus. Special thanks to the many at Optus who spent hours meeting and working with me, sometimes in distressing circumstances and about difficult events. To my knowledge no information was ever withheld, and all are trying to ensure that such an event never happens again.

A team from EY assisted me through the support of a professional secretariat service. Kearney patiently shared their technical expertise with a near novice. My gratitude to both organisations.

Table of Contents

Executive Summary

Just after midnight on 18 September 2025, changes were made to the Optus network that caused Triple Zero calls to fail in South Australia, Western Australia, the Northern Territory and parts of far west New South Wales. The failure lasted almost 14 hours and during that time 605 Triple Zero callers sought to use this part of the Optus network. Of these 605 callers, only 150 successfully connected, leaving the remaining 75% unconnected. Tragically two fatalities have been related to this large number of unconnected emergency calls.

As a result of this incident, the Chairman of the Optus Board, John Arthur, requested that an independent review be conducted. Five matters relevant to the incident were specified for attention:

- the causes of the incident;
- the effectiveness of monitoring and management of Triple Zero calls at Optus;
- whether the recommendations made in a report by Richard Bean, following a major outage at Optus in 2023, had been implemented by Optus;
- whether any aspect of change management and controls relevant to Triple Zero calls gave rise to the incident; and
- the Optus response to the incident.

The full Terms of Reference set are at Appendix A.

The first section of the report examines the causes of the incident in almost forensic detail. Between Optus Networks personnel and their contractor, Nokia, there were at least ten mistakes made. The upgrade of the network being done by Optus and Nokia was not unusual and, indeed, fifteen similar upgrades had been completed in recent months.

The instructions about the change needed for this upgrade, given by Optus to Nokia, were incorrect. Nokia implemented this incorrect change request and adequate reviews of the likely outcomes to follow from this procedure were not made by either Nokia or Optus. The result was a locked gateway implemented at an exchange in Regency Park SA which blocked both voice calls and emergency calls. After a very short period, non-emergency voice calls established alternative paths on the network - it was business-as-usual. Regrettably, this was not the case for the emergency calls, which remained blocked.

It took Optus and Nokia about 13 hours to know of the problem. There were early alerts at the Operations Centre, but these received only cursory attention by Nokia and Optus. There were five calls to the Call Centre, and each caller correctly diagnosed the issue. Their Triple Zero call was not working and the response on the mobile phone was silence. The Call Centre response (after checking that the caller was not in immediate danger) was to try and find a technical problem – either in the caller's device or in the nearby network. The Call Centre had not been advised of any outage and thus assumed that the problem was technical in nature. The issue was not escalated further.

Why the camp-on procedure did not work is a puzzling feature of this incident. 66 callers did camp-on successfully and reach emergency services. Another 84 found an alternative route on Optus and were able to make a successful emergency call. The majority of callers over that 14-hour period did not. What emerged from the behaviour of devices at the time is that for many calls it may take 40-60 seconds to camp-on. In an emergency, people are unlikely to hang on for this length of time, especially when the only response they are getting is silence on the line. There were calls from the same mobile phone models and types that were both successful and unsuccessful.

This raises issues about how well the Triple Zero system is operating and whether it can be improved. It is a highly regulated system that was originally designed in a world of 2G and 3G. Since that time there have been major changes to the networks and devices. Australian networks have essentially disabled 3G and run on 4G and 5G. Devices have become far more sophisticated and new models typically include various changes in their operating characteristics. This report strongly supports more investigation of these matters by both industry and government and welcomes recent changes by the government along lines suggested in the 2024 Bean report. The establishment of a Triple Zero Custodian to oversee the whole system, which relies on many different parties, is especially welcome. And the establishment of a program at University of Technology, Sydney (UTS) to study device behaviour on the networks in different situations is also commendable.

The Bean report in 2024 followed a significant outage at Optus in 2023. Various recommendations were made for both government and carriers to implement. Optus has complied with its obligations and needs to ensure that this continues, especially as more changes are being made, and no doubt will be made in the future. Compliance with requirements should obviously continue, but Optus should further assist government and industry in the near future. This incident has provided valuable new knowledge about device behaviour that should feed into the broader government and industry agenda for the Triple Zero system.

Numerous comments are made concerning governance and process controls at Optus. On the governance front, significant changes have been made at Optus by their owner, Singtel. Over the last year, there has been a move from matrix reporting to the Singtel Group to stronger local management and responsibility. Optus is now led by a stronger local Board, and a new CEO and leadership team have added capabilities to the Optus executive team. These are bold initiatives and despite this incident should continue and be strengthened as needed.

At a general level, risk management must be elevated so that all three lines of defence in risk management are working properly. This is not the case at present. The first line of defence in network operations clearly failed. The second line of defence, which provides independent review and challenge of risk management in the business under a chief risk officer, needs an upgrade in both importance and capability - which is underway. The third line of defence, the Internal Audit function, is currently having its position within the company strengthened, including through the planned appointment of a Chief Auditor who will report directly to the Board. The work in the risk management and audit areas is being oversighted by the two relevant Board Committees at Optus, led by two Directors with appropriate expertise. However, because the local Board has only recently been strengthened, their oversight work, and that of the CEO, has just started.

The other general area where change may be helpful is in Optus' management of contracts for more complex work. This includes the Nokia contract. In some organisations, contracts are handled in a transactional, almost zero-sum, manner where the relationship between the parties is often adversarial. The focus is on costs and not sufficiently on service quality. A better alternative can be a partnership approach in which senior executives of both parties meet once or twice a year to reflect on how the contract is going and whether there are any changes that can be made to the benefit of both parties. While having no firm conclusion as to whether contract management dynamics played a role in this incident, a more cooperative and productive approach may be worth considering.

Optus has been criticised for its slow response in notifying stakeholders, but what can be done depends on what is known. The two main problems were, first, the length of time it took to find the number of calls impacted and their details, and second, the poor information flow internally at Optus because of the siloed working culture.

The process to find the number of callers impacted and their details was slowed by the fact that the failed Triple Zero calls were not carried into the core network. Some complicated engineering had to be done to find this information and awareness of about 100 callers was not acquired until after 8pm on 18 September. By midnight it was clear that over 600 callers had been impacted – about 10 hours after the incident was recognised. Steps have already been taken to expedite this data-finding procedure, noting that its automation is pending.

The other delay was caused by poor internal information flow. Networks were managing the incident during this time, and they should have acknowledged its severity and moved its management to a central Incident and Crisis Management team who operate with a Crisis Communications Team. As a matter of course, these teams maintain appropriate communication across internal divisions, the executive team and external stakeholders. This step was not taken until the morning of the 19 September, when the CEO was informed of both the large number of Triple Zero calls affected and the two fatalities known at that point.

Once the details about callers were found, welfare checks started. The first tranche of 100 checks was done in a timely manner. The remaining welfare checks took longer, as further staff had to be trained to handle the large number of welfare calls.

External notifications can be improved in several areas. Where Triple Zero and emergency services are involved, the States and Territories impacted need to know earlier. Indeed, the same comment applies to any significant outage. There were also cases where email addresses were incorrect (typographical errors and out-of-date information). The team must regularly update their contact register as governments and personnel change frequently. Police at an operational level were contacted as soon as possible and these arrangements worked well. That said, the very large number of impacted callers did pose challenges.

It is important in concluding to note that Optus is at the start of a five-year reform and transformation program. A new CEO was appointed in November 2024 and several additional independent directors were appointed over 2024 and 2025 as part of a program of significant Board enhancement. This degree of change does take time to filter through a large company. The Triple Zero incident provides the opportunity to hasten the transformation and changes needed. While preparing this Report, various possible improvements that could be made have been noted and a checklist of these is included at Appendix C to assist. Calls to replace the current CEO are not helpful at the start of this large program of change and will not help develop the more competitive and reliable telecommunications company needed in Australia. The incident certainly highlights significant problems at Optus that have been evident for some time. Major efforts are now being made to address them. Telecommunications is an essential service, and not only for Triple Zero calls. Optus must recognise their role in serving the community.

Part 1. Causes and Surrounding Circumstances

1. The Incident

1.1 Introduction – three basic questions

On Thursday 18 September 2025, just after midnight (00:17), changes were made to part of the Optus network that caused Triple Zero calls to fail in South Australia (SA), Western Australia and the Northern Territory. A small number of customers in New South Wales near the border with SA were also impacted. Triple Zero services for these Optus customers were not restored until early in the afternoon (14:34) – over 14 hours later.[1]

During this long 14-hour period, 605 callers sought Triple Zero emergency services and assistance of some kind. Of these 605 callers[2], only 150 successfully connected, leaving the remaining 75% unconnected. Tragically two fatalities[3] have been related to this large number of unconnected emergency calls. Three significant questions arise from these failures. The first is why Optus Triple Zero calls did not connect. Emergency calls are an essential service provided by telecommunications companies and people expect that when they need to make an emergency call, they will be connected. The disconnection of Triple Zero calls in this incident was especially puzzling to customers because their usual voice call and other services continued – the outage affected only emergency calls.

Work was being done to install a firewall upgrade at the Regency Park exchange in SA. There is nothing unusual about such upgrades in a network and this was part of a planned program, spread over six months, to upgrade eighteen firewalls. At the time this specific project started, fifteen of the eighteen upgrades had been successfully completed.

The second question is why it took Optus so long to recognise it had a major fault with its Triple Zero emergency service calls. A failure of this kind would usually trigger alerts to the network operators about the problem. Two alerts were indeed detected but the investigation of them did not lead to any corrective action. There were also customer calls to the Optus call centre about Triple Zero call problems. There was no immediate follow-up on this information either. In fact, Optus did not recognise their problem for about 13 hours. SA Ambulance informed the Optus Enterprise division at around 1:15pm that there was an inability to make Triple Zero calls, at which time Optus commenced investigation of the matter. The SA Police followed up this information about an hour later (1:53pm) (as did SA Ambulance again), informing Optus' onshore Emergency and Sensitive Support team.

The third question is why the Triple Zero calls did not all automatically switch to another network or a part of the Optus network that was working. In the event of any network failure – planned or unplanned – Triple Zero calls should automatically divert to whatever network in the area is available. This 'camp-on' procedure failed to complete for most of the Triple Zero calls over that 14-hour period. During that time, 66 Triple Zero callers camped on to alternative carriers and 84 connected elsewhere in the Optus network. These 150 Triple

[1] The use of Triple Zero in this report covers all emergency calls in Australia. These are primarily made to 000, though calls to 112 also fall in this category.
[2] The callers to Triple Zero may have tried to call Triple Zero more than once. For that reason, there is a difference between callers (using a unique person number) and calls.
[3] Optus were told of four fatalities during the hours of this outage but police have informed Optus that two of these are not related to the Triple Zero call outage.

Zero callers were the only successful callers out of the 605 callers that sought Triple Zero services in the impacted area.

1.2 Why Optus Triple Zero calls were disconnected from the network

The disconnection of customers calling Triple Zero was caused by mistakes made by people planning and implementing the upgrade of a firewall. The preparation for the firewall upgrade began on 5 August and a timetable was mapped out to 18 September, when the implementation was due to commence. The type of actions planned were what would usually be expected for a job of this kind. Regrettably, at least ten of these actions were not done properly.

In work of this kind, a detailed Change Request is put together and given to the relevant operations area to implement. The first set of mistakes at Optus were incorrect instructions included in the Change Request sent to the Nokia Network Operating Centre for implementation. These errors appear to be caused by a lack of attention to the matter by the firewall network engineers. Even though some doubt was expressed about the detail of the procedure, the matter was not escalated for further attention.

The firewall upgrade program underway included two types of firewalls - 'demilitarized zone' (DMZ) firewalls and management traffic firewalls (denoted as IX firewalls). In the case of DMZ firewalls, traffic (including voice calls and Triple Zero calls) must be diverted to allow the equipment to be isolated before the work is done. For IX firewalls, this diversion and isolation are not necessary because these are management firewalls that do not directly affect customer traffic. A diversion and equipment isolation can be done to 'err on the side of caution', but it is not strictly necessary – and importantly, if equipment is isolated, traffic must be diverted.

The firewall upgrade in this case was an IX firewall and no traffic diversion or isolation was required or performed, consistent with previous (successful) IX firewall upgrades. Nevertheless, having expressed doubts about the procedure, it was decided by the network engineer to isolate the firewall to err on the side of caution. The problem with this decision was that the equipment was isolated, but traffic was not diverted. While both normal voice calls and Triple Zero calls were immediately impacted, the consequences were different. Voice calls almost immediately found an alternative pathway and their services continued as usual. This was not the case for Triple Zero calls and all these calls were blocked. While about 25% of emergency callers did find another route, and were thus successful, the remainder were not.

Work on an initial implementation plan was begun by the project manager on 5 August and follow-up meetings were scheduled for 8 September. Some network engineers failed to attend these project meetings to assess the impact of the planned work. <u>This was the first mistake.</u>

The project manager contacted an engineer on 8 September after several attempts and held a remote meeting with him to explain the proposed pre-work and the plan. The engineer considered these matters and assumed that the equipment did need to be isolated. He noted some doubt, checked with an engineering colleague, and then decided to 'err on the side of caution' by isolating the equipment with a lock on a gateway before the firewall. On 15 September, he gave approval to the project manager to proceed. A Change Request was then issued to Nokia, the Optus network operator. This direction reflected the project manager's and engineers' work plan, including the blocking of traffic (through a gateway lock in front of the firewall) before work began. This pre-work plan did not clearly include a traffic redirection before the firewall was isolated. This was the second mistake.

The strange thing about this specific Change Request was that in all past six IX firewall upgrades in this program – one as recent as 4 September – the equipment was not isolated and no lock on any gateway was made. Given the doubt being expressed, the issue should have been escalated.

The following diagram depicts the various stages of planning at Optus leading up to the Change Request made to Nokia. This covers the period from 5 August to 16 September.

Figure 1: The Upgrade Project and Engineering Planning at Optus

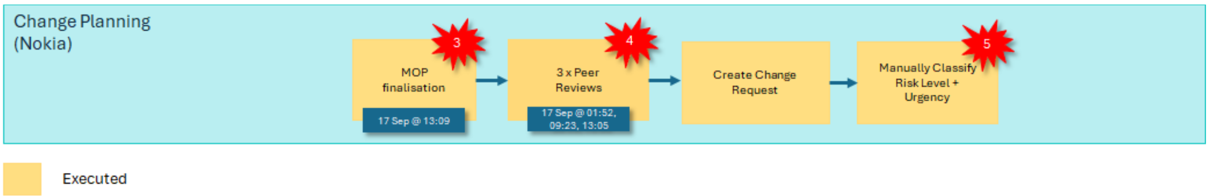
Later, on 17 September, Nokia selected a Method of Procedure to follow to implement the Change Request. This is a very important step because it specifies in detail how the work is to be performed. An incorrect Method of Procedure was chosen. This was the third mistake. For reasons that are unclear, Nokia selected a 2022 Method of Procedure which did not automatically include a traffic diversion before the gateway was locked. It is of interest that on 30 July, Nokia used a correct Method of Procedure for work at this Regency Park exchange on another firewall upgrade. This was for a DMZ firewall that did require a traffic diversion and a gateway lock before work started. Had this method been used, the traffic would have been diverted and then the gateway locked, rather than simply locking the gateway. The decision to place a lock on a gateway without a traffic diversion was a major error but it did reflect the understanding of the Change Request issued by Optus.

Furthermore, the incorrect method chosen was peer-reviewed three times at Nokia, but no one noticed that the critical traffic diversion step had been omitted or that the Method of Procedure selected was not the one used for the prior six successful upgrades. This was the fourth mistake. After the last of these three reviews on 17 September, Nokia asked the Optus engineer about the procedure and was advised to lock the gateway. A few minutes later, Nokia advised the Optus engineer that the work was to commence that night and received no response.

The reason why the work was split into two parts and spread across two nights is not clear. Nokia began the work 24 hours before they planned to complete and in the first step the gateway was locked (on 18 September) and the final step, to upgrade the firewall, was scheduled for after midnight on 19 September. The consequence of planning to take two nights to do the work is not trivial because closing this gateway exposes the Optus network to a significant drop in resilience. Had the firewall upgrade been done over one night (as all other upgrades in the program had been) the gateway would have been locked for a maximum of 6 hours rather than the planned 24 hours or more.

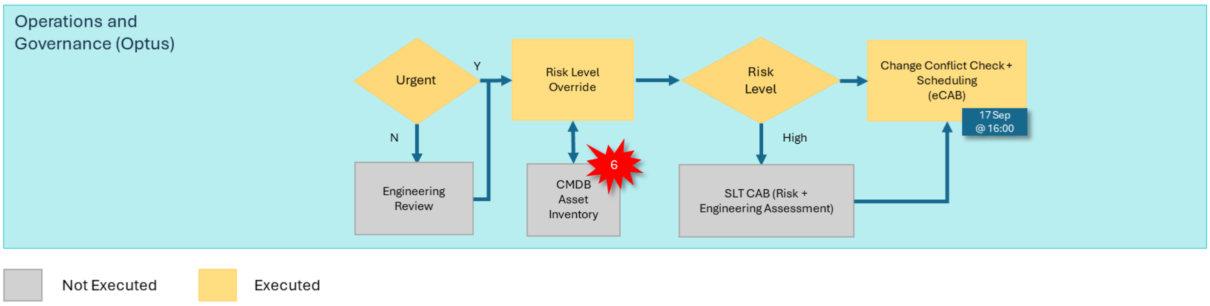
Following the fourth error, the wrong choice for the Method of Procedure, the risk level and urgency of the work were then classified manually by Nokia. Risk was classified as ‘no impact', meaning that there was to be no impact on network traffic, and the firewall upgrade was classified as urgent. This was the fifth mistake. The work was not urgent, and the risk level was certainly not 'no impact'. This stage of the upgrade planning at Nokia is shown in the diagram below.

Figure 2: Change Planning at Nokia for the Upgrade



Following this step, the urgent classification continued. Consequently, an engineering review, which normally would have been conducted, was skipped. Furthermore, when the asset inventory was checked, the platform was not classified there as high risk – as it should have been – which meant that the Change Request was not automatically upgraded to a high-risk classification. This meant that an approval by the senior Change Advisory Board was also skipped. This was the sixth mistake. This part of the process is set out in the figure below.

Figure 3: Operations and Governance of the Upgrade at Optus



Pre-checks were conducted by Nokia in the early hours of 18 September and the upgrade commenced using the incorrect Method of Procedure. This implementation was the seventh mistake. From that moment, at just after midnight on 18 September, emergency calls were disrupted.

There are alerts in the network to signal disruptions. Following the upgrade work, two such alerts were triggered at the Network Operations Centre. The first was at 3 minutes after work commenced (00:20) and the second about 30 minutes after (00:47). In response to the first alert, Nokia linked the alert to the fact that work was being done and did no further investigation. The second alert was evident to the Optus team separately. An incident was created by Optus and escalated to the command centre, with a message questioning whether the behaviour was related to the change underway. Again, no further investigation occurred. This was the eighth mistake.

Post-implementation checks were conducted about two hours after this first implementation step (at 02:40). These checks included examination of graphs which showed that call failure rates were not trending down, as would be expected, but instead were increasing. Yet again, this anomaly was not picked up. This was the ninth mistake. This is shown in the task sequence below.

Figure 4: The implementation Stage at Nokia

Finally, monitoring of Triple Zero calls was occurring at Optus but the method being used was not adequate. The analysis used nationwide aggregate data to pick up the variation in call volumes and this data was not sufficiently granular to enable detection of the emerging problem. This was the tenth mistake. State-based data should have been used or even more localised (regional) data.

In summary then, to answer the first question: the Triple Zero customer calls did not connect to the network during a typical firewall upgrade implemented just after midnight on 18 September. There was a failure to divert voice calls, including emergency calls, before closing a gateway to isolate the firewall at Regency Park exchange in SA. Closing the gateway without a traffic diversion blocked Triple Zero calls. This failure happened because of a series of at least ten mistakes by Optus employees and their contractor Nokia. These mistakes can only be explained by a lack of care about a critical service and a lack of disciplined adherence to procedure. Processes and controls were in place, but the correct process was not followed and actions to implement the controls were not done or not done properly.

1.3 Why It Took Optus So Long to Find the Failure in Emergency Calls

There was information available to Nokia about 13 hours before it was eventually recognised that there was an incident. The first indications were alerts at the Network Operations Centre as noted in the section above. There were two of these alerts: the first was checked by Nokia and not investigated beyond noting that it was related to the firewall upgrade at Regency Park; and the second, in the Network Operations Centre, was notified to Optus and again was simply noted as being related to the firewall upgrade underway. The fact that alerts can be overlooked because they are related to ongoing equipment upgrade work is astounding, when the reason for those alerts may be unanticipated problems caused by that work. Had these alerts been given more than cursory attention, the fact that no traffic diversion was in place should have been picked up. This would have allowed a correction about 30 minutes into the outage.

Spreading the work across two nights instead of doing it all in one night also exacerbated the problem. Had the work been completed in one night the closed gateway would have had an impact for about 6 hours and not the 14 hours that was experienced. There would have been some Triple Zero calls with connection difficulties but far less than those experienced across the 14 hour period.

There were also calls to the Optus Call Centre. There were five calls between 10:13 am and 2:11pm on 18 September indicating that Triple Zero calls were not working. There was a process in place for the call centre operators to deal with a Triple Zero call failure. First, the caller was asked 'is there an immediate danger?'. A positive response was to be immediately connected to the Emergency Call Person. All five calls received at the call centre did not involve immediate danger and hence were not connected to the Emergency Call Person. They were also not escalated within Optus – although, after dealing with the calls, the receivers did try to get to the bottom of the problem by speaking to technical expert staff and/or putting the caller through to a technical person.

Reviewing the response to these calls is sobering. Every caller diagnosed their problem accurately. They could not connect to Triple Zero and the response on their mobile phone (and other phones tried at the time) was one of complete silence. Because no 'red flags' had been signalled to the call centre to alert them of any network incident, and as no significant outages had been declared, the reaction to the calls was to assume some local network issue or problem with the device. None of these five calls was escalated to more senior levels by either the call centre staff or the technical people that tried to work out the cause of the individual problems.

One caller who needed assured access to Triple Zero assumed his/her device was not working properly and sought assistance to find the nearest retail outlet to purchase a new mobile phone. All other callers were even more distressed as they had just experienced a medical emergency with a friend or relative and had tried multiple devices to reach Triple Zero. Their calls were made to alert Optus to the problem and to complain about the service. The response involving a search for a technical solution between them and the call centre operator was inappropriate at that time and is emotionally wrenching. At least one complaint was understandably lodged with the Telecommunications Industry Ombudsman.

Calls to the Triple Zero call line were not checked until 1:31pm on 18 September, when Optus made several test calls. This followed the SA Ambulance notification to Optus' Enterprise and Business area of the issue. At 1:51pm, a major incident was declared. At 2:20pm, Optus verbally instructed Nokia to unlock the gateway at Regency Park Exchange, and at 2:31pm the gateway was finally unlocked.

Because of the failures at both Nokia and Optus to investigate the two alerts in more than a cursory manner, and because of the inadequate process at the call centre for handling Triple Zero call failures, the earlier warning signals went unheeded. It was only when made aware of the problem by SA Ambulance (and then SA Police) that Optus investigated. Initial estimates suggested a low number of Triple Zero callers were impacted, but as the call log was examined further the number was quickly increased to 605 callers experiencing Triple Zero call failures. Welfare checks were begun as callers were identified but this follow-up was slow. The main reason was the long time it took Optus to identify the unsuccessful callers. Because the calls were not carried into the core network, some complicated engineering was needed to locate the telephone number of impacted callers and their details. Improvements have since been made to this tracking procedure to speed it up.

Once aware of the problem, Optus rectified the matter within minutes. The real tragedy here was the duration of the Triple Zero call outage and the failure of Optus and its contractors to deal immediately with the warning signals they received. At Optus and Nokia, the necessary processes were in place, but their requirements were not performed properly. At the call centre, the problem was a process that did not necessarily escalate the Triple Zero call difficulties of customers.

1.4 Why Most Triple Zero Calls Failed to Connect to Optus and Other Networks

The answer to this third question is the most complex. As noted above, in a network outage – both planned and unplanned – Triple Zero calls from mobile phones are supposed to automatically switch to the nearest carrier available. This could be another pathway on the caller's carrier or on another carrier. In this case, of the 605 Triple Zero callers affected by the outage, only 150 found an Optus pathway or camped on to another carrier. Of the 150 callers that were successful, 66 camped on TPG or Telstra and 84 used the Optus network.

Normal voice calls and Triple Zero calls behave differently. In an outage of this kind, normal voice calls are successful after a very short time. The device (usually a mobile phone) initially fails because its primary voice gateway is unavailable. The device then quickly re-registers on a secondary voice gateway and attaches to the network. The device then stays attached and voice calls are successful.

Triple Zero calls are different. Each call requires a call registration to be made, and when the primary voice gateway is unavailable, the device chooses some other option. What option is chosen appears to be influenced by the characteristics of different mobile devices, timing settings in the network, and how these factors interact. This does not seem to be solely an Optus problem.

At the time of the incident, the only difference between the Optus network and other telecommunication networks was the different 'emergency time-out' setting. This setting (timer) controls how long an emergency call remains actively attempting to connect. The emergency inactivity timer at Optus was set at 10 seconds, down from the previous 600 seconds, following regulator concerns that Google Pixel 6A devices running Android 12 were unable to reconnect to Triple Zero after failed emergency calls. Google advised users to upgrade to Android 13, which resolved the issue, but Optus also reduced their emergency inactivity timer to 10 seconds to enable faster retries after call failures.

We understand that other carriers have longer time-out sets that may range from 150 to 600 seconds. It appears that the 10 second timing setting in the Optus network was the only significant difference between Optus' network and other Australian networks for Triple Zero behaviour. Since this incident this time setting has now been changed by Optus to 600 seconds.

The characteristics of many different mobile devices when they call Triple Zero is being analysed at Optus[4] to better understand device behaviour. Not surprisingly, this preliminary work shows that different mobile phone brands and models behave differently. At this early stage, the focus has been on Apple and Samsung devices as they are the most common devices used on the Optus network. The test results below are preliminary only.

Apple devices in the laboratory showed the following call pathways:

- Where they were rejected 'appropriately' before 10 seconds, they connected to a second IP (Internet Protocol) address and successfully called Triple Zero.

---

[4] The University of Technology Sydney (UTS) is also investigating device behaviour but this work is in its early stages.

Where there was no response in 10-12 seconds, they looked for a 3G connection, but since 3G has been disconnected they then either connected to another mobile operator or continued to search for 3G. The devices that continued to search for 3G were not always successful in connecting to Triple Zero and those that connected successfully took 40-60 seconds. With such a long delay in an emergency call, it is unlikely that a caller will patiently wait.

Samsung devices were different. They all tried to connect to a second IP, whether appropriately rejected (within 10 seconds) or not, and they all tried to connect to 3G.

- Those calls that had been 'appropriately' rejected within 10 seconds connected to another mobile network operator and then successfully connected to Triple Zero. During their route to success, they had set up a second IP and tried to find a 3G connection.
- Those calls that tried to set up their second IP after 10 seconds failed and so moved to try and connect to 3G. Some of these calls found the public land mobile network and successfully reached Triple Zero - although it again took 40-60 seconds to connect. Others were not successful.

In summary, mobile phone brands and types have different properties – different operating systems, software, firmware, hardware and timing mechanisms. Differences in user behaviour may also have had some impact – in particular, how long callers were prepared to wait to connect and where callers were located when the call was made.

1.5 Comment

Three issues are clear during this incident. The first is the very poor management and performance within Networks and their contractor, Nokia. Process was not followed, and incorrect procedures were selected. Checks were inadequate, controls avoided and alerts given insufficient attention. There appeared to be reticence in seeking more experienced advice within Networks and a focus on speed and getting the task done, rather than an emphasis on doing things properly. This behaviour must be rectified to ensure that such mistakes are not repeated.

The second problem was at the Call Centre. Instructions to operators did not recognise that they may be the first alert channel for Triple Zero difficulties. This matter has now been rectified, and further changes are ongoing to address the issue as discussed further in Section 2.3.

Finally, the important issue of the camp-on failure to complete for Triple Zero calls during this outage is most troubling and possibly one for the entire industry and community. This is a technical matter that the industry and government must investigate further – and as soon as possible. Emergency calls that take 40-60 seconds to connect are not ideal and the community must be made aware of the issue. Furthermore, the fact that 3G is now essentially discontinued in Australian networks may have caused an impact on different devices that is more extensive than initially expected.

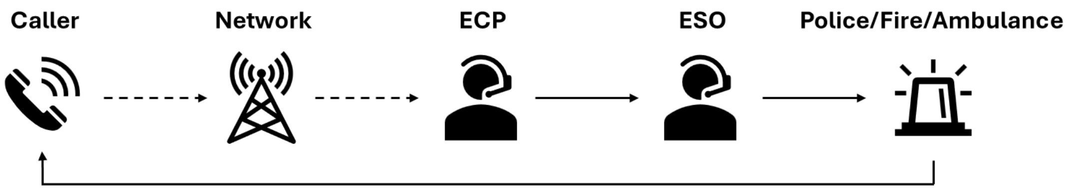
Part 2. Management of Triple Zero Calls

2. Triple Zero Call management

2.1 The Triple Zero Service

Triple Zero is a free service that enables voice calls to police, fire and ambulance services in an emergency. It is intended to be available at all hours of the day. The service is provided by telecommunications companies and emergency service organisations in each state and territory. The service is backed by legislative, regulatory and contractual arrangements.

When a person dials Triple Zero, the call is transmitted by the carrier, Optus in this case, to the Emergency Call Person (ECP). A recorded announcement advises the caller that they have dialled Triple Zero and will be connected to an operator. The ECP then asks ‘Police, Fire, or Ambulance?’ and for the location details from the caller. The ECP then connects the call to the relevant Emergency Service Organisation (ESO), along with information to identify the caller’s location. The process is depicted below in a simple diagram used in the Bean Report.[5]



The ECP service is delivered by Telstra under a contract with the Australian Government. The voice-only ECP service has obligations in its contract that largely mirror the ACMA requirements in an *Emergency Call Service (ECS) Determination 2019 (Compilation 3, dated 28 October 2024)*.[6] Basically, the ECP must answer 85% of the calls within 5 seconds, and 95% within 10 seconds.

A text-based emergency service, via teletypewriter, is provided by Concentrix, the current National Relay Service provider. They are the nominated Emergency Call Person for the 106 emergency text services available for people who are deaf or have a hearing or speech impediment.

The emergency services provide ‘answer points’ to the ECP. These ‘answer points’ engage with the emergency callers and facilitate the dispatch of the appropriate emergency service in response to the life-threatening or time-critical emergency. ESOs are covered by relevant State and Territory legislation specifying how they are managed and operated. It is of note that ESOs are increasing their use of data and can, for example, ask callers to send photographs in cases (like an accident) where this can assist in the service to be provided. The voice-only nature of the ECP and the increasing use of data by ESOs suggest that the

[5] Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Review into the Optus outage of 8 November 2023 – Final Report, March 2024. Richard Bean.

[6] This Determination is made under subsection 147(1) of the *Telecommunications (Consumer Protection and Service Standards) Act,1999. Compilation 4* was released on 1 November 2025. Commentary in this report relates to the compilation in effect at the time of the incident.

voice-only feature of the ECP is worth examining in the future. The extension of the service to one that is data-enabled does have advantages but is not necessarily straightforward.

2.2 The Legislated Requirements for Triple Zero

The legislated requirements for carriers, including Optus, are also set out in the ECS Determination. The requirements cover notification, cooperation and welfare checks in the event of a significant outage.

The intent of the Determination is to ensure the highest level of access, integrity and service continuity for emergency calls. To enable this outcome, all carriers must provide the following six Triple Zero service features.

1. Access: Emergency calls must be free of charge, and the carrier must ensure that its network allows access to Triple Zero calls even without an active number in service.
2. Carrying Emergency Calls: The carrier must ensure the emergency call is carried to the relevant termination point on its network or, where this is not possible, it must use another telecommunications network by camping-on.
3. Highest Priority: Any Triple Zero call must have highest priority over all other calls. The carrier must not introduce delays during the carriage of an emergency call (for example, through a recorded message).
4. Minimising Non-Genuine Calls: The carrier must take steps to minimise non-genuine Triple Zero calls, including monitoring the quantity of calls, having a documented process, and cooperating with the ECP and relevant ESO.
5. Awareness: The carrier must promote awareness to its customers and the public generally, about the emergency call numbers, that it is a free service, and that emergency calls can always be made.
6. Location Information: The carrier must, as far as practicable, ensure that it automatically carries information about the public number that made the emergency call. On request it must supply the ESO with the most precise possible location of the emergency call. There is also a non-binding guideline to set technical standards for the ‘most precise location information available’ for emergency calls.

There are also requirements relating to customer devices. If a device cannot carry an emergency call, either on the default carrier or by camping-on another network, then that device is ‘not configured’ and specific obligations apply.

- For existing customers, the carrier must use its best endeavours to identify any devices that are not configured to be able to access the emergency call service, either through the carrier or camp-on.
- If a device is not configured, the carrier has five business days to notify existing customers of the issue and must do so at least two more times. They are also obliged to disconnect the device from the network in 28-35 days and inform the customer that this will occur.
- For new customers, the carrier must identify whether their mobile phone is configured to be able to access emergency call services at the carrier or by camp-on. If the mobile is not configured, then the end-user should be informed of alternative devices that are configured appropriately. No service must be provided to a mobile phone that is not configured to be able to make emergency calls.

There are also obligations for the carrier if any network changes and testing are proposed that could impact emergency calls. The firewall upgrade that caused this incident was not expected to cause any disruptions to emergency calls. If any disruption to emergency calls was expected, then Optus would have been obliged to test that emergency call functionality would be maintained – either elsewhere in the Optus network or through camp-on.

There are also obligations on carriers in the event of a 'Major Outage' or a 'Significant Local Outage'. The definition of these types of outages is related to the number of services affected and their duration. As soon as possible after such outages, the carrier must conduct welfare checks on the safety and well-being of any caller whose emergency call has failed. At a minimum, the person must be contacted by a call or through at least two messages. If these efforts are unanswered, the relevant state or territory police must be contacted to allow them to check if the caller needs assistance. There is also best-practice industry guidance about the conduct of welfare checks after an unsuccessful emergency call. While the incident did not meet the criteria for mandatory welfare checks, Optus did conduct such checks.

Following an outage, the relevant carrier must also test its camp-on functionality so that calls on its network are able to camp-on other networks. Similarly, the carrier must provide camp-on services to other networks.

Carriers also must comply with regulations concerning information sharing with ACMA about their outage, minimise the impact on emergency calls during the outage, and meet various disruption protocols.

2.3 Managing Triple Zero Calls at Optus

The management of Triple Zero calls involves testing of devices and networks to ensure that the emergency call service is working for customers using properly configured devices, as well as device testing to ensure that all devices being carried on the network are configured to enable the service.

To test Triple Zero functionality, Optus routinely makes limited test calls to the ECP from different locations in its network at agreed times so as not to impact the operations of the ECP. This method of testing is in the process of being upgraded. Automatic testing is being implemented, which makes Triple Zero calls on a continual periodic basis by state. Testing is also done after upgrades and other work on the network and after outages.

The level of testing being done prior to this incident was clearly insufficient to find the complex Triple Zero call behaviour of devices present in the 18 September incident. While the testing regime met requirements, the 'clunky' manual approach now being upgraded by both the ECP and Optus allows testing to be more frequent at more locations and automatically handled. This testing does not affect ECP functionality and is expected to be ready by the end of the year. Optus has increased its manual testing program in the meantime. While this testing improvement is welcome, it is unlikely to pick up all the complex device behaviour noted in this incident.

The other network matter that Optus has now examined is its timing settings. As noted above, Optus had a 10-second timing set, which was considerably less than other networks. Following the incident, Optus has changed this timing to 600 seconds.

Optus maintains a list of devices (arranged by their Type Allocation Code) which have demonstrated issues with Triple Zero calls. Optus uses this 'banned list' to comply with regulation and to make sure it can provide emergency services to its customers. However, this incident demonstrates that making sure devices are properly configured for Triple Zero calls is challenging. And as commented earlier, this issue is not likely to be only an Optus one. There are several concerns:

- Older devices may have once been configured correctly but changes in the networks may mean these devices are no longer able to reach Triple Zero. As mentioned earlier, the biggest change to the network in recent times has been the closure of 3G, and the impact that this has had on devices may be more widespread than originally estimated. The issue needs further investigation by both the industry and government agencies.
- Some devices are correctly configured but may not connect for 40-60 seconds, during which time the caller hears only silence. When distressed, a caller is unlikely to wait for that length of time. This delay also needs further investigation and action. At the very least, the community must be made aware of the issue.
- There are likely to be some devices that have never been correctly configured. They may have been bought on-line or in a market where they have never been tested for Australian standards. Suppliers of devices must self-declare compliance to be able to sell mobile phones, but formal oversight and checking of such declarations are weak and no formal compliance database is kept at present.

These matters do need to be addressed immediately to give more confidence to customers about the integrity of the Triple Zero call system. Recent changes announced by the government to address some of them are noted. The Minister has also requested that a database of compliant devices be set up. Recommendations from the Bean report are also being implemented.

Customers should be encouraged[7] to test their own devices for Triple Zero calls and, if in doubt, raise the matter with Optus. It is critical that this is not used as a device-selling opportunity but, rather, to provide and assure service. It is notable that Telstra has recently written and messaged its customers to check Triple Zero call functionality on their devices.

If a device used by an existing customer is not configured, there are requirements for Optus to follow as noted above. These include the obligation to provide information about alternative and properly configured devices (including low-cost options).

The second feature of Triple Zero call management concerned the call centre, where management of Triple Zero calls was clearly not acceptable. As noted, Optus has made immediate changes to its procedures so that any call about Triple Zero or an emergency number is immediately escalated to a leader. A number of these more highly trained people are present at the call centre in high-visibility uniform and easily located. Offshore staff also now have some Australian Optus employees joining them. In a short period of time more change will occur. Optus is also moving part of its call centre back to Australia and operating that service in Australia 24/7, to which end recruitment is underway. Both these measures will improve the call centre response.

On the network side, changes are being made in two areas – at the Operations Centre and within actual network process and procedures. The Operations Centre at Optus has several levels – Nokia carries out several levels of operations offshore under contract and Optus manages the other levels in Australia. All Operations Centre work is to move to Australia and its level of automation is to be increased. This decision was made in May of this year, before the Triple Zero incident, to give Optus more direct oversight and control of such an essential part of its business. This incident simply emphasises the importance of this change and the

[7] This advice is contrary to Section 31 of the ECS Determination to 'take steps to minimise non-genuine calls'. It is noted, however, that all major carriers appear to be pursuing this course of action.

need to expedite it. It will take time and is being planned and escalated where prudent to do so.

The lack of care and work discipline evident in all the mistakes that were the cause of this incident is more difficult to address. There have been recent changes at the executive levels and there is growing awareness of the siloed structures within networks and between networks and other business units. These silos may have contributed to the lack of transparency within the engineering groups and less comfort in seeking advice or escalating when needed. There are reasonable processes and procedures, but they must be actioned properly. The networks area must understand its importance as a service provider as well as its source of technical expertise. This means better risk management at their network business unit level where risk, *inter alia*, involves maintaining emergency service provision. It is an understatement to say that risk management at that business level was materially deficient during this incident.

Finally, welfare checks are an important part of emergency call management. In a major or significant local outage, a carrier must check on the safety and well-being of a caller who has failed to connect to emergency services. At a minimum, this check involves contacting the caller through a call or at least two messages. If these contact methods go unanswered, a call to the relevant police is made to enable a further check.

The handling of welfare checks in this incident should have been timelier but as noted the delay was caused by both the length of time taken to locate caller details and by the need to train more staff to handle the large number of calls. Attempts were properly made by Optus to call all unsuccessful Triple Zero callers. The calls were scripted. Once well-being was ascertained, the cause of the outage was explained in some detail if the customer wished. Of the unsuccessful calls, some were contacted by Optus, and the remainder were passed to the relevant police to check on. The dealings with police in SA and WA were challenging because of the large number of callers involved. Optus consulted with emergency services where fatalities occurred and offered to visit those families if they wished. This process was completed by Optus and for family privacy reasons no further information on it is available.

2.4 Comment

The Triple Zero system was designed in the days of 2G and 3G. It is possible that standards and regulations - and the system as a whole - have not kept up with the changes in the network since then and the greater sophistication of devices.

It must be recognised that very few callers use fixed lines, and software and other settings are no longer simply embedded in networks. Devices have different characteristics, and each connects with the network settings of different carriers. The system is more decentralised. Furthermore, as reliance on devices increases (and not only for Triple Zero calls), reliable connection is all the more critical.

The Triple Zero system is based on voice calls at present, even though many emergency services are using data services extensively. It may be worth exploring whether Triple Zero should also allow data services.

Finally, as noted, more investigation is needed at a sophisticated technical level about the relationship between different mobile phones and their network. There is work underway at UTS about mobile phone behaviour, assisted by both government and industry. This work has only recently begun and there is no doubting its importance. It is also important that such work examines scenarios that include the situation where voice calls are working but Triple Zero calls are not, as well as full outage scenarios.

The standards and requirements for both devices and carriers to ensure that emergency calls are successful may not have kept up with the many changes in devices in recent years. This incident suggests that current arrangements are not fully reliable, and it is of concern that many devices take up to 40-60 seconds to connect. This delay is something that customers at all telecommunications companies should be informed about. While Optus and its contractors were the cause of this incident, they do not determine the different way that devices behave, and this matter must be addressed.

Part 3. Implementing the Bean recommendations

3. The implementation of the Bean report recommendations

3.1 The Bean Report

Following a nationwide outage in the Optus network on 8 November 2023, a review of the incident was conducted by Richard Bean for the Australian Government. The outage lasted for about 12 hours and had a major impact on all Optus customers. Critical services were also interrupted, including those of government, public health and safety infrastructure.

The focus of the review was on five matters:

1. The functioning of Triple Zero calls during the outage and whether changes are needed to ensure access to Triple Zero at all times. (The areas where changes may be required were noted as technical settings, regulatory requirements, the role of other networks, and the interactions between carriers and other participants in the telecommunications sector.)
2. The role of Government in managing and responding to national service outages.
3. The adequacy of requirements for customer communications.
4. The adequacy of customer complaint processes and compensation.
5. Any other implications for the telecommunications sector.

The review made eighteen recommendations for change (see Appendix B). Nine relate to changes for Government to carry out; six are changes for both Government and Optus (and other carriers); and three are specifically directed at Optus (and other carriers).

Gaps and flaws in the Triple Zero call system are identified and the review aimed to make changes that would limit outages and their impact. Noting that outages will inevitably occur, the review also focussed on making the Triple Zero service robust, ensuring the key players know their roles, and ensuring that customers and the community are well informed and have appropriate complaint and compensation processes if needed. Finally, they aimed to better prepare government, community, organisations and businesses for outages that inevitably occur.

The nine recommendations for government to carry out are not relevant to this report but are worth noting. They are likely to impact Optus in the future and are set out below:

- Set up a Triple Zero custodian body to oversight the entire Triple Zero system.
- Review the government contract for the delivery of the Emergency Call Person service (performed by Telstra).
- Set out clear and detailed requirements for carriers to notify government of service disruptions and how communications and collaboration with other carriers, Ministers, various agencies and relevant parties should occur.
- ACMA should develop a standard or determination about what information carriers should give their customers during outages.
- The Department should further develop and promote initiatives to the community to assist and recover from outages caused by natural disasters.
- Complaint-handling standards and record keeping should be amended to ensure they cover network outages.

- An industry-wide standard should be developed about the resolutions available for customers affected by a crisis or a large-scale outage. (Possible compensation and penalties should be addressed.)
- Governments should review their own arrangements for maintaining operations and critical services during an outage.
- The Department and ACMA should review all legislation and regulation relating to Triple Zero in the light of all these recommendations and the outcome of ACMA's investigation of the Optus outage.

The six matters that were for both government and carriers concerned various measures to be taken by government, but which clearly needed input from carriers and close consultation and collaboration with them.

These were recommendations about Triple Zero functioning (Recommendation 1), information sharing between carriers (Recommendation 5), outage reporting (Recommendation 6), and expansion of the current protocol to cover all obligations arising from a disruption (Recommendation 7).

The work already underway for roaming during natural disasters is recommended for expansion to cover temporary roaming during outages (Recommendation 14). And finally, the government should require that mutual assistance arrangements are set up between telecommunications service providers to assist in managing and resolving outages (Recommendation 15).

There are three recommendations for the attention of Optus and other carriers. First, to carry out six-monthly end-to-end testing of their Triple Zero system. This should cover network functionality and capability, device behaviour, and interoperability on all parts of the Triple Zero system. Deficiencies were to be reported to ACMA, along with a remedial plan (Recommendation 3). Second, if this testing does not include devices supplied by the customer, then those customers should be informed that their devices have not been tested in an emergency scenario (Recommendation 4). And third, network operators must establish the ability to remotely access and use network management tools and have sufficient redundancy to deploy them in the event of a core network failure (Recommendation 16).

The Government accepted all eighteen recommendations, though they did note that the recommendation to establish a Triple Zero Custodian needed further investigation (Recommendation 2). They also agreed only in principle to extend the work on roaming to temporary roaming during outages. They note that implementation may not be feasible due to mobile network capacity (Recommendation 14).

The timing for the implementation of the recommendations varied. Some were not to be applied until 1 November 2025 (technically after this outage, but in this incident, Optus met the new reporting requirements).

3.2 The status of implementation at Optus

The status of Optus' implementation of the Bean recommendations has been reviewed internally and Optus reported to the regulator that its matters had been addressed. Recent changes by the government will activate those recommendations that are the joint responsibility of carriers and others (including government) in the Triple Zero system. These matters must be carefully attended to by Optus and assistance should be given to all the parties in the Triple Zero system to fulfil their roles. In this context, the experience of Triple Zero operations during the incident is valuable information that should be shared with, *inter* *alia*, the UTS group that is testing devices and with the Emergency Call Person to enable more automatic testing of Triple Zero functionality.

Recently, Kearney has been engaged by Optus to review, among other things, the Optus response to the Bean Report. They agree with the internal assessment that the recommendations have been implemented but note that further improvements are possible to go beyond the regulated requirement. For example, the recommendation to conduct end-to-end testing of the Triple Zero system every six-months (Recommendation 3) has been met, but this incident highlights that more attention is needed to become more effective. As noted, Optus is working (with the Emergency Call Person) to automate the checking system so that more testing can occur from more locations and more frequently. This is now implemented. At present, calls to Triple Zero can clog up the Emergency Call Person and affect the running of emergency calls. The Triple Zero system does involve many parties and allowing more automatic testing is only one facet. Recent changes by the government, including the appointment of a Triple Zero Custodian to oversee the system, will assist with a more thorough oversight of the entire system.

If devices that customers supply have not been tested for Triple Zero functionality, then Optus is obliged to warn customers that those devices have not been tested in emergency scenarios (Recommendation 4). Optus does keep a list of devices that are not configured appropriately for the network, and these are on a banned list and cannot be connected to the network. This process does not capture so-called ‘grey’ devices that have been bought online or overseas and may not be compliant. Self-declaration by such device suppliers is not likely to be a strong enough requirement to ensure that these devices are compliant. What this incident highlights, however, is that some devices did successfully call Triple Zero and some that were of the same make and model did not. The reasons for this device behaviour must be investigated. For example, did some callers wait on the silent phone longer and thus got connected? Were some callers better located and why?

The ability for network operators to remotely access and activate network management tools and have sufficient redundancy to deploy them in the event of a core network outage (Recommendation 16) has been met. This incident highlighted another network issue in that it did take an unacceptable length of time to identify the number of callers who were unsuccessful in getting through to the Emergency Call Person.

EY did a detailed examination of the welfare check process at Optus in May 2024, following the significant 2023 outage. In that incident there were some Triple Zero calls that were unsuccessful, and Optus failed to identify all those callers and therefore missed conducting a small number of welfare checks. EY reviewed the processes and controls in place for welfare checks and made recommendations for improvements. EY then later assessed that these recommendations had been implemented.

The welfare check process during a significant network outage entails two areas of responsibility – the Networks Team and the Frontline Team. The Networks Team is responsible for the infrastructure necessary for emergency calls and ensuring that accurate and timely extraction of customer data is made so that welfare checks can be made. The Frontline Team is responsible for making the welfare checks with customers and, where necessary, escalating the issue to the relevant state or territory police. The Frontline Team must also maintain detailed records of these checks, and their outcome, for accountability and later tracing if needed.

The detailed results of EY’s investigation in 2024 showed one shortcoming in the controls applied to the welfare check process - the lack of a formal training plan and monitoring thereof. The training sessions for welfare checks were *ad hoc*, with the consequence that updated improvements to the process were not always known or understood. The risk with this *ad hoc* training approach was that there could be a lack of awareness about the latest standard operating procedures and regulatory requirements. Recommendations were made to address that problem and an assessment made within three months found that the matter had been addressed.

3.3 Comment

The Bean Report recommendations followed Optus' significant 2023 outage. While Optus has met its requirements, it is important for Optus to not only comply with the regulations but to extend actions further to increase their effectiveness. Furthermore, because many of the recommendations have only been recently implemented, Optus should use its experience to assist and provide input to the Department of Communications, UTS (where devices are being investigated), ACMA and the new Triple Zero Custodian. This recent outage has provided valuable information about the behaviour of the Triple Zero system, and this should be shared.

Part 4. Processes and Controls

4. Change Management Processes and Controls Relevant to Triple Zero Calls

Much of this topic has been covered in earlier sections discussing the incident. However, there are four more general management processes at Optus that are relevant and have not been directly dealt with elsewhere. These are:

- the transition underway at Optus, independent of this incident;
- risk management;
- contract management; and
- essential service provision.

4.1 The Transition to Reform Optus

In recent years Optus has had a series of significant incidents:

- a cyberattack in 2022;
- a major outage in 2023; and
- an ACCC-related court finding of unconscionable conduct related to inappropriate sale practices between August 2019 and July 2023.

In an attempt to ensure that such incidents do not happen again, or that they at least are better managed when they occur, important changes have been made. The owner of Optus, Singtel, has fundamentally changed a matrix reporting structure through to the Singtel Group to a stronger local management structure. This entails a corresponding significant strengthening of the local Board, with broader responsibilities that are limited only in relation to a few prescribed matters (matters that in a public company would typically be referred to shareholder owners for approval). In addition, a new CEO has been appointed, who reports to the local Board.

New executives and leadership changes have occurred with the aim of adding to capability, and it is notable that many of the people interviewed for this report have only been at Optus for a very short period. The changes underway will take time. The focus of the transition is on three things:

- Strengthening the resilience and reliability of the network. (Amongst other things this means a redirection of investment expenditure towards the network, partly at the expense of sales and marketing.)
- Streamlining complex IT architecture and critical platforms to reduce complexity for employees and customers.
- Working urgently to improve processes, the need for which has been highlighted by this incident.

Progress is being made, but transitions of this magnitude take time, and this Triple Zero outage amplifies the need for change and where possible the need to hasten its implementation.

Moving to stronger local management is a correct step given the many differences between Australia and other geographies in relation to telecommunications. Consideration should be given to strengthening this move by adding to the competency and skill base of the local

Board and ensuring that the CEO and executive team have sufficient authority to execute the approved transition strategy.

4.2 Risk Management

Risk management typically follows a ‘three lines of defence’ model:

- Line 3 is the operationally independent audit function led by the Head of Internal Audit – it assesses the adequacy with which Line 1 and Line 2 perform their designated roles and the associated risk outcomes. The Chief Auditor reports to the Board.
- Line 2 is a structurally and operationally independent control function led by the Chief Risk Officer - it independently reviews Line 1’s risk profile, management and outcomes and challenges this work. The Chief Risk Officer reports directly to the CEO.
- Line 1 is the risk management in the organisation and all its business units. The business unit is accountable and responsible for identifying, monitoring and managing its own risks as well as its control environment and outcomes.

It is an understatement to note that the three lines of defence model is nascent at Optus.

In this incident, the first line of defence clearly failed. Within business operations in the Networks area at both Optus and Nokia, processes were not followed properly, and controls were skipped, ignored or/and not properly checked.

This raises the question of whether the second and third lines of defence at Optus are adequate or also in need of improvement. Responsibility for the second line of defence lies with the Head of Risk Management and the risk management team. This team has until recently been staffed with an insufficient number of experienced and capable risk managers, and its impact has been limited. Where they did have useful contributions and suggestions to give to line 1 (Networks in this case), they lacked the authority to do so effectively. A new Chief Security and Risk Officer has just been appointed, reporting directly to the CEO, and the greater responsibility and impact that this team should have is now being pursued. The immediate aim is to pivot from piecemeal responses to issues to a more elevated and systematic risk management approach. Initially the focus is on three objectives:

- to change the operating model and who does what in relation to risk;
- to uplift risk capability and maturity across Optus, assisting business units to reduce risk where it is outside the organisation’s appetite; and
- to uplift controls assurance activities as a matter of urgency, particularly for Networks, Cyber and Regulatory Compliance.

The line 2 team has recently documented a set of high-level risk types that are understood at both the Executive and Board levels. These risk types provide a useful reference point for risk management and audit planning activities, although they are one component among many that will be needed in the planned risk management uplift at Optus.

It is recognised that the third line of defence, Internal Audit, needs to build and strengthen its operations in line with the broader uplift underway in local governance and risk management. Internal Audit has appropriately focussed on high-risk areas and identified many of the issues raised in this report. However, it has not had a sufficiently elevated position within Optus to ensure that its concerns and recommendations led to sufficient action and appropriate implementation. To address this, the Optus Board is in the process of filling critical positions and establishing a Chief Auditor role.

These changes are being firmly supported by both Singtel and the Optus Board. In addition, the Board Audit and Risk Committees are working well together, and both Committee Chairmen know their subject areas and roles well. Along with the recent significant efforts by the executive team, improvements are clearly in train.

4.3 Contract Management

The third issue of note is contract management. The way that the Nokia contract is managed has been interesting to observe and the view that this contract could be better managed is preliminary and based on this limited experience only. It does appear that morale in the offshore Operations Centre is poor in comparison to many other similar operations. This would not be conducive to questioning mistakes made by Optus network engineers when noticed.

Optus has a reputation in Australia for being transactional in its contracting. This almost zero-sum game approach does contrast with the style of partnership often evident in other organisations where large and complex operating environments (like the Nokia Operations Centre) are involved. With a partnership approach, among other constructive practices, the parties meet regularly every six months or so at a senior level (sometimes the CEOs) to discuss any changes that may be beneficial for both and any innovations that may be sensible to consider.

Optus might consider whether it would see benefits from moving to this style of contract management for complex matters. It does encourage contractors to offer their best staff, and it can lead to more cooperative outcomes.

4.4 Essential Service Provision

Finally, a culture within Optus that focusses on its role as an essential service provider should be fostered. Telecommunications is now, without doubt, an essential service that the community relies upon for all types of things – banking, medical records, important contact details, payments and, of course, Triple Zero calls. While frontline staff dealing with customers are aware of this importance, those staff who are not dealing directly with customers must remember the importance of what they do in providing this service. At present, this customer-centric focus is not sufficiently embedded.

4.5 Comment

The incident provides increased motivation to pursue the changes underway and to do so as fast as possible without impacting the quality of outcomes. The significant change in management structure is a bold step and should be continued and strengthened where needed. Singtel is a leading global communications company and the temptation to get directly involved when an incident of this nature occurs must be immense. To date, no such direct involvement is apparent, and faith has been maintained in the local Board, the CEO and executive team – holding to this position seems the best course of action at present.

Measures must be taken to improve risk management. At the first and second line of defence, it has been poor, and third line strengthening is underway. This incident highlighted the shortcomings.

Whether or not contract management needs improving on the lines suggested for consideration is for Optus to investigate. Examining the nature of contract management at Optus is beyond the scope of this assignment, but the way Nokia performed and behaved does suggest improvements may be needed.

Finally, the need for an essential service provision culture is important. Over time, the digital world has become almost as important to the community as water and power – and any outage at Optus has similar consequences.

Part 5. Response and Notifications

5. The Optus Response and Notifications

5.1 A General Note on Incident Management

The reality is that all utilities have unplanned incidents from time to time, with varying degrees of severity. There is typically a well-rehearsed way of dealing with them. Initially the severity of the incident is assessed, and this determines whether a relatively routine incident management team is set up or, for a severe incident, a crisis management team is established. Relatively routine incidents are usually managed in the relevant operational part of the business, and the rest of the company may well remain unaware of the matter until there is a general briefing of incidents that have occurred throughout the week or month. However, as a routine type of incident unfolds it can be escalated as more is understood about its impacts and level of severity. This escalation is not unusual for major crises as it often takes time to know what is happening.

When an incident is serious, the management is led by a specialist crisis management team that is trained and well-rehearsed to handle the matter across the company. The management of the incident moves from a local basis to a central coordinating role. The crisis management team coordinates all the activities that are required. These include but are not limited to: gathering all information about the incident; ensuring that the cause is fixed or its effects ameliorated; ensuring any safety issues are attended to; understanding the time needed for the many tasks involved and coordinating their operations; checking that those who need to know about the incident within the company do know; and ensuring that required external notifications are made. The crisis management team does not do these tasks but makes sure the right people/team are taking responsibility and doing their jobs, and that they are being done in an appropriate order.

At Optus a very long description of how to manage a crisis ran over more than 40 A4 pages. This covered various plans and scenarios for different types of events. There are two obvious problems with this approach. First, in a crisis no one is going to examine or read over 40 pages, and second, a crisis is not usually like what has been anticipated and planned.

A crisis is best managed by an experienced and calm leader armed with a short checklist and a small team of trained staff who have the capacity to adapt to the circumstances as they unfold. Fortunately, a recent change in crisis management has begun, following a prescient paper to the executive team that outlined the problems with the existing approach. As well as addressing the two issues mentioned above, the paper noted that Optus was going through a major organisational change and role clarity in response to an incident was not clear. The current business ‘silos’ structure made coordination difficult, and more training and rehearsals were needed. Changes to the crisis management approach were requested and approved and this reform is underway.

5.2 The Optus Response

Responses depend critically on what is known. This section sets out ‘who knew what when’ before commenting on what happened. In this event the initial responses were relatively routine at a local level within Networks. The causes of the Triple Zero outage have been set out in Section 1 and this section begins at the time Optus became aware of the issue.

An incident ticket was raised at 1:32pm on 18 September (about 13 hours after the start of the problem) when the Enterprise business requested an investigation. This followed several calls about 8 minutes earlier (from SA Ambulance) that noted an apparent Triple Zero issue with mobile calls in SA. The incident ticket at 1:32pm was raised appropriately within the Optus system for further investigation.

Networks quickly made test calls to Triple Zero and about 20 minutes later a Major Incident was declared. At this point the internal communications were between Networks and the Enterprise team that had raised the issue. The fact that the Call Centre had been dealing with a small number of callers with Triple Zero issues had not been reported at this time, and this knowledge of issues with Triple Zero calls had not been recognised as an indicative warning of an outage.

Minutes after Optus had declared a Major Incident, the SA Police reported the matter to the Emergency Services Support team. The Corporate, Regulatory and Government Affairs division became aware of the matter at this point. They requested information from Networks, and the executive team (including the CEO) was notified of what was known at that time – an issue with Triple Zero calls in SA. This team notified the Emergency Call Person about what they knew at that time.

By about 2:30pm on 18 September, the knowledge within Optus was limited to the fact that there was an issue. They did not know how many Triple Zero calls had been affected or the phone numbers linked to any such calls. Networks began to address the cause of the problem, and an order was given to unlock the closed gate. Once this occurred, the operation of Triple Zero returned to normal, but the impact of the incident remained unknown. Efforts to identify how many callers had been impacted, and their location and phone numbers, began. At this time, there was insufficient understanding of the event to increase the severity rating of the Incident, and it continued to be managed by Networks at a relatively routine level.

At around 2:30pm, Networks estimated that there were 10 unsuccessful Triple Zero calls in WA and SA. Welfare checks were completed later in relation to these calls as it took a long time for the contact details to be obtained. Because the callers had not connected into the core network, some complicated engineering was needed by Networks and Nokia to track the calls.

The Call Centre requested information from Networks about the outage as there was no detail in the Digital Case Management system, and similar updates from Networks were requested by Corporate, Regulatory and Government Affairs. The Emergency Call Person and Concentrix were updated and ACMA was informed of a 'Significant Network Outage'. Technically, the outage did not then meet the definition of a Significant Network Outage (due to the low number of calls impacted), but ACMA was informed because of the Triple Zero calls involved in the outage. Executives and the CEO were updated by Networks at a meeting at 5:30pm. The estimated number remained at 10 unsuccessful callers to Triple Zero, though work continued to identify further missed calls.

It was not until about 8pm that 100 failed Triple Zero calls were identified. Welfare checks began once phone numbers were identified and these contacts were completed at 9:33pm. Where contact could not be made, the numbers were referred to police to complete the check following the usual arrangements. Meanwhile, Networks continued to search for the number of unsuccessful callers.

At this stage, the incident was still being managed by Networks. In retrospect, there is no doubt that Networks should have escalated the severity of the incident at this point. They knew that the number of Triple Zero calls emerging was likely to increase above the 100 identified at this stage. The need for other areas within Optus to know what was happening was also clear – the Call Centre and Corporate, Regulatory and Government Affairs had already sought updates.

An escalation in incident severity classification, and informing the CEO, would have seen management of the matter moved centrally to an experienced Incident and Crisis Management Team with its Communications Team. Had this occurred, information flows within Optus would have improved and the required external notifications, including a press conference, would have happened hours earlier. Unfortunately, knowledge at this point, on the evening of the 18 September, was limited to those areas that Networks had informed about the 100 unsuccessful Triple Zero callers – the Call Centre (which had begun to run the welfare checks) and Corporate, Regulatory and Government Affairs (which was providing information to the Emergency Call Person, ACMA, relevant Police, the Minister's office and the Department).

In retrospect, either of the executives leading these two areas could have alerted the CEO to the 100 unsuccessful Triple Zero callers at this time. However, neither had the knowledge that Networks possessed, and the welfare checks on the latest tranche had not begun. The Call Centre was waiting for details about caller phone numbers, and both executives were waiting for accurate information about the number of unsuccessful calls (which Networks was continuing to check) and the outcome from welfare check calls that had just commenced. The search process for unsuccessful callers was refined by the engineers, and it was not until about 11:30pm that evening, 10 hours after knowing of the outage, that the data for the remaining calls were obtained.

It is important to note that the first fatality related to the outage was known through a welfare check at 8:43pm and a second was known about 15 minutes later through another welfare check. Call Centre staff at this point knew about the 100 unsuccessful callers, but they did not escalate their knowledge of the potential fatalities to the leadership at this time. The response at the Call Centre seems to have been one of panic and distress, and it was not until 2 hours later (at 11:06pm) that an offshore Call Centre Leader was informed of the situation. About 20 minutes later, an internal email from the Call Centre provided an update on the welfare checks process and noted two potential fatalities. This email was sent to middle managers at Optus, but its contents were not known until Australian waking hours at 5:22am. The managers immediately noted that a meeting at a senior level was needed, and this occurred at 6:21am on the morning of 19 September. It was at this point that the knowledge of potential fatalities reached senior executives, at which time further detail was requested. This delay in the flow of information from the Call Centre is unacceptable, although it has since been addressed.

To address the issue, significant changes have been made to the Call Centre operations. Leaders in the Call Centre are now clearly visible in the workplace and readily available for assistance. Any issue with a Triple Zero call is immediately raised with a leader who has the skills to manage the matter and escalate it to senior executives as required. In addition, a larger component of the Call Centre operations is to be established onshore to complement the offshore operation. At the time of this event, the small onshore part of the Call Centre was not a 24/7 operation. This proposed increase in onshore operations and an extension of their hours to 24/7 will take some time and recruitment to enable these changes has commenced.

Actions in the following hours were expeditious. The CEO was informed, the first Crisis Management Team session was held, an Incident and Crisis Communications Team session was held, an executive team meeting was set up, and external notifications commenced. The communications procedure for a crisis follows from the establishment of the Incident and Crisis Communications Management Team and necessarily involves Emergency Services, the Chairman, Minister and her department, relevant Premiers, Singtel as owner, the Board, ACMA, the TIO, and not least the customers and general public.

The welfare checks on the remaining calls did not commence until about 12 noon the next day (19 September), after data on the final tranche of calls was validated and additional training was provided to those staff doing the welfare checks. The very large number of calls meant that the usual complement of staff for welfare checks was not adequate, and more staff had to undergo training. These welfare checks were completed in about 2 hours, and unsuccessful call data was provided to police at around 4:30pm.

Further data on unsuccessful calls was found as Optus went back and checked its processes. Because of this work, another 7 unsuccessful calls were identified on 22 September and welfare checks made.

The delay in finding the number of unsuccessful callers and their details significantly hampered the management of this incident. A near-accurate assessment of the number of callers impacted was not available until the afternoon of 19 September. This held up welfare checks, progress updates within Optus, and external notifications. Further information continued to be obtained over the next two days.

The delay in obtaining details about the unsuccessful calls is being attended to by putting in a digital case management system. This is intended to assist with tracking normal voice calls, but it will also automatically trigger welfare checks when a Triple Zero call failure is detected. This means the need to manually search for data will be removed and the information required will be available sooner. However, while this system is in readiness testing it is not yet live, and its implementation must be seen as urgent.

5.3 Notifications

There are major improvements that can be made to Optus' notifications and two criticisms that have been publicly offered are correct. The first related to the tardiness in letting the public know of the Triple Zero call outage and the fact that some callers were unsuccessful. The reason for the lengthy delay in letting the community know about the Triple Zero outage was simply the length of time it took Optus themselves to realise there was a problem – and, because of the difficulty in identifying caller numbers and details, it took a very long time to assess the extent of the outage.

As noted in Section 1, the numerous mistakes made by network engineers added hours to the outage and as a result added hundreds to the number of callers impacted. Had the firewall upgrade not been planned to be split over two consecutive nights, the incorrectly locked gateway (with no traffic diversion) would have been locked for about 6 hours at most, and not the 14 hours that were experienced. Over the space of those 6 hours (even allowing for the mistakes in the procedure), there would have been some Triple Zero calls blocked, but nowhere near the numbers that occurred.

Similar comments can be made about the alerts, checks and controls that were not given appropriate attention during this initial work. Had these been attended to properly, the outage may have lasted less than an hour and impacted very few emergency callers.

The other major factor in the delay was the siloed way of working that was particularly evident in the Networks and Call Centre areas. Management of the incident was done by

Networks. The Call Centre and Corporate, Regulatory and Government Affairs requested updates needed for their work, and the provision of such information is not routine for Networks. This became very clear once the number of calls impacted increased.

Indeed, as noted above, once the number of emergency callers impacted rose, accompanied by the likelihood of more to come, the severity of the incident should have been escalated. This would have meant the centralisation of its management, including communications. The decision to move management of the incident from Networks to a central Crisis Management Team should have occurred at about 8pm on 18 September if not earlier. This would have brought external notifications, including the public media announcement, forward by about 4-5 hours. The press conference would have been around noon the next day, rather than in the evening. While the exact number of unsuccessful callers was not known in the morning, it was known with sufficient accuracy at 10am, when the estimate was 624 callers impacted. Two fatalities were also known by that time, although welfare checks were continuing.

The Call Centre silo was particularly evident. It had not escalated the five calls received noting difficulties in connecting to Triple Zero. These occurred on 18 September, four of the calls being between 10am-12:30pm. Had Optus made test calls to Triple Zero at that time, knowledge of the outage would have been obtained. (In the Call Centre's defence, escalating Triple Zero call problems was not part of their specified procedure at that time, although it is now.) The Call Centre did not share their knowledge of two potential fatalities until just before midnight and this notification was ineffective. It was by email only and to middle management personnel at Optus. As a result, the email was not seen until early morning in Australia and only then quickly escalated to the executive team. There was no knowledge of potential fatalities at the Executive level until the early morning of 19 September.

The second criticism about notifications came from the State Premiers. They, along with the NT Chief Minister, were not contacted until after the press conference on 19 September in the early evening. This was far too late, given that the understanding of the incident at Optus was approaching reasonable accuracy in the early afternoon and the knowledge of fatalities in SA and WA. When an outage affects emergency services, the States have an immediate interest, and Optus must recognise the importance of the States and Territories in this area beyond the operational level. While Optus was notifying and contacting the relevant police, Premiers and Chief Ministers needed to be informed as soon as possible about the areas of their population that experienced the difficulties and, when possible, what constituencies were covered. This is even more important in those States where fatalities occur.

The lack of immediate connection between Optus and the states and territories was exacerbated by the difficult time of day (Friday evening) and may also have reflected a lack of familiarity with Optus contacts. If the latter is the case, then the matter should be addressed. Verbal contact was made in due course, and the CEO did eventually speak to the Premiers in WA and SA.

By comparison, the notifications to the Australian Government were better, though not without some errors. Notifications began once information about the outage was known and updates continued steadily. The one glitch appeared to be the use of an outdated email to contact the Department of Communications initially. This was soon rectified.

The contacts with ACMA appear to have been what would be expected. and the notification of a Significant Network Outage was appropriate though not formally required. Updates were provided as information became available and as required.

Notifications to the Emergency Call Person and Concentrix were initially timely, but the full extent of the outage does not appear to have been conveyed to these stakeholders until after the CEO's press release.

Notifications to the police were also what was required; however, the large number of welfare checks needed was unusual for the police, and both SA Police and WA Police sought clarifications about the process. This emphasises the need for clear communication and directions to the State police when routine welfare checks are far more in number than might have been expected. The clarification was given quickly and the police provided good, cooperative service.

A detailed timeline of the notifications can be found in the Optus submission to the Senate Standing Committee on Environment and Communications. In less detail, the notifications that occurred once the CEO knew of the fatalities and that the number of unsuccessful callers to Triple Zero exceeded 100 follows:

Friday 19 September

- 8:13am – CEO learns of fatalities and increasing numbers of unsuccessful Triple Zero calls.
- Within 2 hours – informs Optus Director, Yuen Kuan Moon (also CEO of Singtel), as the Chairman (John Arthur) is not in an appropriate time zone. Sends text to the Chairman and informs other Optus Board Directors.
- 2:36pm – CEO updates ACMA on fatalities found during welfare checks.
- 3:00pm – Short Optus Board meeting before media conference planned for late afternoon.
- 3:49pm to 4:33pm – Contact with Department of Communications and Ministers Office – update and notice of upcoming media conference.
- 4:36pm – Media informed of upcoming press conference.
- 5:45pm – Press conference.
- 5:51pm – Emergency Call Person advised of press conference.

Throughout this day, there were also numerous calls to police to refer welfare checks in all states and the Northern Territory. Most were in SA and WA, with a small number in NSW and NT – and several callers with addresses in Queensland and Tasmania. Over the next 5 days, further checks and verifications were conducted, and updates provided as required.

5.4 Comment

There are several matters to highlight for improvement in Optus' response and following notifications. The first is the necessity to attend to the siloed way of working so that information can flow easily around the company. This will take time as there is a significant cultural dimension to address. The Call Centre has already taken steps to ensure that Triple Zero matters are escalated, which is important - but across the whole company there needs to be a recognition that silos must communicate.

Second, Optus must learn from its mistakes so that this type of event does not ever happen again. Networks must pay attention to processes and the controls applied to them. To have a standard firewall upgrade go so badly is inexcusable. Execution was poor and seemed more focussed on getting things done than on being right. Supervision of both network staff and Nokia must be more disciplined to get things right.

While changes to incident and crisis management have recently been approved, further training, rehearsals and exercises are needed. This applies especially within Networks. They need to know when to move from managing a network incident locally to central management of that incident. Routine incidents can unfold into incidents that need central management and communication skills. Networks are not equipped to manage an incident that needs coordination across the company and good internal and external communication.

The system being put in place to enable more efficient and faster tracking of normal voice calls and Triple Zero outages should be activated as soon as possible.

In relation to notifications, each relevant team must ensure it has up-to-date contacts for all its external stakeholders. These obviously include the regulator, the Australian Government Minister and Department, and the Emergency Call Person, but they also include the Chief of Staff for all State Premiers and Chief Territory Ministers. This information needs constant refreshing and checking routinely as governments and personnel change. It would also be wise for Optus to work more closely with the States, given the importance of telecommunications and emergency services. Notifications appears to run smoothly at an operational level (including for fires, floods and cyclones), but the executive team should also become more familiar with the States at levels above the operational.

Appendices

A. Terms of Reference

The terms of reference for the Independent Report are:

1. identify the facts in respect of the causes of, and circumstances surrounding, the Incident including in respect of:

    (a) Optus’ applicable processes, protocols and operations; and

    (b) relevant aspects of the Triple 000 system, including why Triple 000 calls did not connect to emergency services or move (“camp-on”) to another network;

2. review Optus’ operational management of Triple 000 calls in the Optus Network, and in particular the monitoring and operational effectiveness of Optus' handling of Triple 000 calls, in so far as it related to the Incident;

3. review the steps taken by Optus to enact or comply with the recommendations of the review conducted by Mr. Richard Bean, former Deputy Chair of the Australian Communications and Media Authority, after the nationwide Optus outage in November 2023;

4. review the change management processes and associated controls in the Optus Network relevant to Triple 000 calls and any aspect which gave rise to the Incident; and

5. review Optus' response to the Incident and the notification of relevant regulatory authorities and emergency services, and the appropriateness of actions taken and escalation of the Incident, having regard to Optus’ crisis management policies and procedures and legislative requirements.

Noting that the Independent Report is expected to be made public, to the extent that any aspect of the proposed Independent Report gives rise to concerns regarding national security, is privacy protected information or would result in the potential disclosure of commercially sensitive information (such as network architecture), then such material will be managed as a separate confidential disclosure to Optus outside of the Independent Report.

B. The Bean Report Recommendations

Terms of Reference 1 – Functioning of Triple Zero

1. Mandatory requirements should be put in place, by augmenting existing requirements or otherwise, to:
   - More clearly and explicitly articulate precisely what is expected of network operators in regard to ensuring calls are delivered to Triple Zero
   - Include specific obligations that network operators wilt towers in the event of loss of connectivity to a core network, ensuring calls to Triple Zero can be carried by other networks.
2. Establish a Triple Zero custodian, with oversight of and overarching responsibility for the efficient functioning of the Triple Zero ecosystem, including monitoring the end-to-end performance of the ecosystem.
   There are a number of ways this could be achieved, including by establishing a new body or enhancing the role of an existing body. It would not be a regulatory function: where matters were identified for change, existing bodies would be responsible for implementation.
3. To ensure (to the extent possible) continuous access to Triple Zero, carriers must conduct 6-monthly end-to-end testing of all aspects of the Triple Zero ecosystem within and across networks. The end-to-end detection testing should include:
   - Network functionality and capability during outages of various types
   - Behaviour of all known devices in different circumstances
   - Interoperability of all parts of the ecosystem (from originating carrier, to Emergency Call Person (ECP), to Emergency Service Organization (ESO) answering point) during outages.
     Any identified deficiencies must be reported to the ACMA and be accompanied by a remediation plan with timetable.
     This requirement should be mandated in a standard or determination.
4. If this testing does not include devices supplied by the customer (i.e. ‘Bring your own device’) then information should be provided to those customers warning that those devices may not have been tested in emergency scenarios.
5. Require carriers, through a standard or determination, to share real time network information detailing outages with relevant emergency services organisations and other appropriate entities, including the body referred to in Recommendation 2.
6. Require providers, through a standard or determination, to report to the ACMA and the Department, within a mandated timeframe after a major outage, detailing its causes, steps taken to resolve it, the impact on Triple Zero, and a clear and detailed plan, with timeline, to address issues identified and avoid similar outages in the future.
7. Combine and expand existing disruption protocol instruments to cover all matters relevant to outages in any element of the Triple Zero ecosystem.
   There are currently multiple obligations related to actions taken during and after network disruptions. Combining these obligations in one document and ensuring they cover the system from end to end would greatly improve understanding and clarity of responsibility.
8. The Department should review the contract under which Triple Zero is delivered, with a specific focus on the central role of the ECP within the ecosystem.

The review should consider, in light of the recommendations of this Review relating to the Triple Zero ecosystem, including Recommendation 2, governance structures, and separating financial matters from other ECP obligations.

<u>Terms of Reference 2 – Role of government in managing and responding to a national service outage</u>

9. The Protocol for Notification of Major Service Disruptions (the Protocol) should be improved and augmented with clear and detailed requirements for Government communication and collaboration during telecommunications outages through a central coordination point in Government.
   This should cover communication and collaboration with carriers, relevant Ministers, Commonwealth, state and territory government agencies, the Telecommunications Industry Ombudsman (TIO), the Australian Consumer and Competition Commission (ACCC), ACMA, Emergency Service Organisations (ESOs) and other relevant parties.
   The Protocol should also be closely aligned with the Australian Government Crisis Management Framework (AGCMF) and the National Coordination Mechanism (NCM).

<u>Terms of Reference 3 – The adequacy of requirements for customer communication in national service outages</u>

10. The ACMA should develop a standard or determination requiring carriers to communicate specific information to customers during and about outages. The Communications Alliance Emergency Communications Protocol – Industry Guideline G663:2022 or one or more of the carriers' existing internal communications protocols could be used as a base but there needs to be an explicit focus on communications between the affected network provider and its customers as well as other stakeholders.
11. The Department should develop further and promote the educational initiatives developed in 2020-2022 to assist the public, businesses and other organisations to prepare for and recover from outages as a result of natural disasters. These materials should be reviewed and enhanced to apply to a broader range of scenarios including major network outages. The Department should promote these materials to the community.

<u>Terms of Reference 4 – Complaints and compensation</u>

12. The Complaints Handling Standard and related Record Keeping Rules should be amended to ensure they account for the impacts of network outages and that the definition of complaint in the Standard meets community expectations in relation to crisis events.
13. An industry wide standardised approach to the form of resolutions available to consumers affected by a crisis or large-scale outage should be implemented.
    This standardised approach should address the possible forms of compensation and penalties applicable to loss of service during outages, enabling the TIO to address mass events without requiring large numbers of individual complaints, investigations and resolutions. While it is not intended that this measure replace the Customer Service Guarantee (CSG), it could provide a similar framework through which outages affecting more than fixed line voice services are considered.

Terms of Reference 5 – Other: Resilience and interdependencies

14. Work currently being undertaken on roaming during natural disasters should be followed by work on temporary roaming during outages caused by other events, such as those which occurred on 8 November 2023. That work should be undertaken with reference to international experience as to cost and feasibility.
15. The Australian Government should require mutual assistance arrangements to be established between telecommunications service providers during outages to assist in managing and resolving those outages, learning from international experience (for example, similar to the Canadian MOU).
16. Network operators should be required to establish the ability to remotely access and activate network management tools, and have sufficient network redundancy to deploy them, in the event of a core network outage.
17. Australian governments should review arrangements for maintaining their operations during outages including telecommunications redundancy for critical government services. Consideration should also be given to maintaining this information in a central repository.
18. The Department and the ACMA should institute a review of all legislation and regulation relating to Triple Zero, with a clear focus on the recommendations of this Review and the outcomes of the ACMA's investigation regarding the Optus outage.

C. Checklist: Possible Improvement Measures

Numerous measures for improvement flow from this report, which the Optus Board and management may wish to consider and implement.

For Networks

1. Ensure that there are controls to support the robust execution of the correct processes and procedures when making routine changes within the Networks area.
2. Encourage Network staff to escalate any issues outside their immediate group if they have doubts and would benefit from more experienced oversight.
3. Expedite the move of the entire Operations Centre onshore as much as is prudently possible.
4. Conduct incident management exercises at Networks to improve their judgement about when to escalate an incident to a more severe level. A routine incident can develop a higher level of severity and Networks must recognize what role they can play and what is best delegated elsewhere. Where central management is needed, the management control must shift from Networks to the Incident and Crisis Management Team and its related Communications Team.
5. Expedite the implementation of the system to enable faster tracking of caller details in the event of an outage for voice calls and/or Triple Zero calls.
6. Monitor the recent change to the 'emergency time-out' mechanism to ensure that the 600-second timing now set remains the most appropriate.

For the Call Centre

7. Continue the improvement processes underway at the Call Centre, including the deployment of visible senior staff with whom matters can be raised and the movement of further Call Centre operations onshore (including some 24/7 operations).

For the Triple Zero System Generally

8. Recognising that this incident has provided useful information about device behavior, assist the government, the Department, the new Triple Zero Custodian, UTS, ACMA and the wider telecommunications industry with the further work needed on device behaviour.
9. Encourage investigation of whether making the Triple Zero system data-enabled is worth doing.
10. Inform all customers that their devices may take 40-60 seconds to connect to Triple Zero and encourage them to test their devices to ensure they work for a Triple Zero call. To ensure that the Emergency Call Person does not get unnecessary calls, set up a system where devices can be tested. This is an industry-wide matter and best done as an industry-wide initiative.

For General Optus Management

11. Continue with the significant transition to reform underway and use this incident to learn and hasten change where possible.
12. As noted, an effective first line of risk management was not evident within Networks through this incident. This must be addressed to avoid further incidents.
13. The second line of defence, the internal risk management team that reviews and challenges risk management practice in the business, is in the process of improving and must gain the seniority and capability it needs.
14. The third line of defence, Internal Audit, needs to build and strengthen its operations in line with the broader uplift underway in local governance and risk management.
15. Consideration should be given to contract management at Optus, especially for complex and essential services, and whether or not service quality could be improved by a less adversarial approach.
16. Address the siloed nature of work at present at Optus and facilitate a shift to a more cooperative, company-wide way of working. This has a cultural dimension and will take some time.

For Notifications

17. The team with responsibility for external notifications should consider a closer relationship with State and Territory governments above the operational level of emergency services. As telecommunications is now an essential service, this level of government is increasingly important.
18. This communications team should update their list of contact details frequently.

For the Optus Board

19. To strengthen the recent move to more local responsibility, the Board should consider the adequacy of its skill base and depth and, if appropriate, make the changes needed.
20. Oversight the efforts already commenced to upgrade risk management in all three lines of defence and assess whether these are sufficient by the standards of a large and complex organisation in a critical industry.
21. Ensure that the CEO and executive team have sufficient authority and delegations to manage the approved transition to reform.