Investigation Report into the Triple Zero Service disruptions of 4 & 26 May 2018.

October 2018

Contents

Abbreviations and acronyms

Abbreviations and acronyms	Full description
ACMA	Australian Communications and Media Authority
BCP	Business Continuity Plan
CA	Communications Alliance
CAD	Computer Aided Dispatch
Carrier	Telecommunications Carrier
CFA	Country Fire Authority
CLI	Calling Line Identification
CMT	Crisis Management Team
CNR-IVR	Caller No Response - Interactive Voice Response
CSP	Telecommunications Carriage Service Provider
DRM	Disaster Recovery Manual
ESAP	Emergency Service Answering Point
DOS	Denial of Service
DoCA	The Department of Communications and the Arts
ECLIPS	Enhanced Calling Line Identification Processing System: Telstra's emergency call handling and management system
ECP	Emergency Call Person: Telstra is the emergency call person for Triple Zero and 112 as specified by the *Telecommunications (Emergency Call Person) Determination 1999.*
ECS	Emergency Call Service: As defined in the *Telecommunications Act 1997.*
ESO	Emergency Service Organisation: Police, Fire or Ambulance
ICEMS	Inter-CAD Electronic Messaging System
IP	Internet Protocol
IPND	Integrated Public Number Database: Database of telecommunications customer information in Australia, arranged by number, for all carriers and carriage service providers.
IVR	Interactive Voice Response
MIM	Major Incident Management
NECWG-A/NZ	National Emergency Communications Working Group – Australia and New Zealand
NG000	Next Generation Triple Zero
PSA	Public Safety Agency
PSTN	Public Switched Telephone Network

Abbreviations and acronyms	Full description
PushMoLI	Push Mobile Location Information
RVA	Recorded Voice Announcement
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSA	Standardised Mobile Service Area
Telco Act	*Telecommunications Act 1997*
TCPSS Act	*Telecommunications (Consumer Protection and Service Standards) Act 1999*
TIPT	Telstra IP Telephony
Triple Zero	000 and 112
TUSOPA	Telecommunications Universal Services Obligation Performance Agreement
TZCC	Triple Zero Coordination Committee

Executive Summary

Telstra is the Emergency Call Person (ECP) for the delivery of Triple Zero Emergency Call Service (ECS) in Australia and has been for over 50 years. Telstra is under contract with the Australian Government for the delivery of the ECS and is also subject to regulatory requirements under the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (TCPSS Act) and relevant determinations under the TCPSS Act.

This investigation sets out the Department of Communications and the Arts' (DoCA's) assessment of Telstra's service outage that affected Triple Zero calls on 3 & 4 May 2018 (the 3 & 4 May Outage) and a separate incident on 26 May 2018 (the 26 May Incident). The investigation takes account of information provided by Telstra, including reports on the 3 & 4 May Outage provided on 15 and 30 May and 27 July 2018; Telstra's response to further queries in relation to the 3 & 4 May Outage and the 26 May Incident; and input from State and Territory Emergency Services Organisations (ESOs) and telecommunications carriers.

These disruptions to the Triple Zero Emergency Call Service are the first known disruptions since the Commonwealth entered into contractual arrangements in 2012. Under the TUSOPA, Telstra is required to meet a number of regulatory benchmarks related to the delivery of the service. Since the commencement of the TUSOPA, Telstra has met all of these benchmarks. DoCA recognises that the historical performance of the service has been high, and that today's telecommunications environment involving delivery of services over PSTN and IP networks has created a more complex environment for the operations of the ECP. The events detailed in this report have provided learnings to ensure the service continues to meet the high expectations of the Australian community.

Service disruption on 3 & 4 May 2018

On 3 and 4 May 2018, Telstra experienced a number of issues in its network resulting in disruptions to services, including calls to Triple Zero. As a consequence, some people trying to call Triple Zero either could not get through to an operator, or got through to an operator but experienced delays in being transferred to the appropriate ESO. Telstra conducted welfare checks on calls that could not get

through to Triple Zero. Telstra reached out to all those people it was aware of, who may have been impacted by the incident. DoCA recognises that there may be individuals impacted by the service outage that have not been brought to its attention at this time.

The outage was due to a number of causes, including:

- a partial failure of an inter-state transmission device;
- a fire that caused the cut of an inter-state fibre optic cable;
- previously unidentified software faults in two sets of Internet Protocol (IP) core network routers (that should provide redundancy for parts of Telstra's IP network, services and systems).

It was the combined effect of these three events that resulted in the service disruptions experienced by callers to Triple Zero. Telstra advises that the combination of these events presented a highly unusual and complex scenario involving Telstra's PSTN network, IP network, and physical damage to infrastructure from a fire that was outside Telstra's control, which made technical diagnosis and resolution of the disruptions difficult.

Incident management and stakeholder communication

Telstra has indicated that it has major incident and other operational and business continuity procedures in place, and that these were followed on this occasion. Telstra does not consider that its procedures were inadequate, but advised that it had never had to manage an incident of the magnitude and complexity experienced on 3 and 4 May. Telstra has committed to update relevant procedures to ensure that, if service disruptions occur, communication to stakeholders is improved.

DoCA recognises that Telstra endeavoured to handle the service outage in accordance with its existing procedures, however those procedures were not adequately detailed, nor had they been previously tested under these circumstances, such that they would provide a sufficient response for the community during an outage of this scale and impact.

There were indications of problems with Telstra's network on 3 May. If the Telstra alarming system had recognised the significance of the alarms indicating a partial transmission loss, there may have been an opportunity to restore transmission on the coastal route before the Orange fire disrupted the inland route. This may have prevented or minimised the significant impact to the Triple Zero service that arose on 4 May. Telstra advises it has a number of programs to continually improve its operational support and alarming as technology develops, and has already made some improvements to better identify the significance of such alarms and the associated impact on Triple Zero services.

Problems with existing procedures were evident in Telstra's communication of the incident with ESOs and telecommunications carriers as the incidents unfolded. While Telstra has advised that it contacted ESOs, ESOs advised that in some cases they were left to initiate contact with Telstra themselves to troubleshoot the issue, and in some cases were unable to successfully contact Telstra. In other cases, little or no information was provided by Telstra to ESOs regarding the cause of the outage, the severity of the outage, or expected timeframes for resolution to enable ESOs to properly implement their own backup plans for handling calls and communication to the public. Telecommunications carriers similarly identified insufficient communication from Telstra during the outage. This limited their ability to inform their own customers as to what was happening, or to coordinate and assist Telstra with diagnosis of the outage or the impact of the outage on Triple Zero.

Telstra acknowledges improvements are needed in the area of crisis management across jurisdictions, and, in collaboration with National Emergency Communications Working Group Australia/New Zealand (NECWG-A/NZ), has commenced development of Triple Zero Disruption Protocols with affected

stakeholders. Telstra has cooperated fully and transparently with DoCA throughout its investigation of the incident and in the compilation of this report.

Service Incident 26 May 2018

On 26 May 2018, an unusual volume of calling activity was made to the Triple Zero ECS. This was generated by an attempted international toll fraud event. The unusual calling appeared at the time to be a Denial of Service (DOS) attack, as the calls had the attributes and impact of a DOS event, and actions to prevent further impact to the service were undertaken. The calling activity resulted in congestion of the service, with 158 genuine callers to Triple Zero potentially unable to reach an operator (these callers hung up while in the queue to be answered by an operator). Telstra identified these callers and undertook welfare checks to ensure the safety of callers (one carrier followed up its own customers directly), with no detrimental impact to callers identified.

The incident was managed in accordance with the *Communications Alliance Emergency Call Service Requirements Guideline (G644:2011) (Denial of Service Attack)*, which supplements the *Communications Alliance Emergency Call Service Requirements Code (C536:2011)*. Communications Alliance has commenced reviewing the guideline after this incident to ensure it remains fit for purpose. It should be noted that the guideline is a controlled document not available to the public.

DoCA observed improved communications during this incident compared to the 3 & 4 May Outage, with ESOs receiving regular updates throughout the event on 26 May. DoCA also observed improved collation of call data to undertake welfare checks compared to the 3 & 4 May Outage. Telecommunications carriers however indicated frustration about a lack of communication from Telstra until up to eight hours after the unusual calling volumes ceased.

The recommendations contained in this report proposing improved communications between the various parties, therefore relate to the experience of stakeholders dealing with Telstra during the events of 3, 4 and 26 May.

A separate investigation into Telstra's compliance with the Triple Zero regulatory framework is currently being conducted by the Australian Communications and Media Authority (ACMA). That investigation has not yet concluded.

Recommendations

The recommendations set out in the report are as follows:

1. That communications from the Emergency Call Person (ECP) to Emergency Service Organisations (ESOs), public safety agencies, telecommunications carriers, carriage service providers, media, other government stakeholders and Ministers are improved through the development of Triple Zero Disruption Protocols. Development of these protocols should be led by the ECP, and approved by members of NECWG-A/NZ and the Department of Communications and the Arts (DoCA) Triple Zero Coordination Committee.

2. That Telstra finalise its review of its network alarm systems and take action to ensure that "loss of communications" alarms are actively identified for rectification.

   Note: Telstra has already implemented the following actions to meet this recommendation:

   - *automated tickets of work to initiate incident restoration activities;*
   - *implemented alarm collection system improvements to allow correlation of alarms to parent alarms, and refining of alarms to provide improved visibility for network managers; and*

- *utilising big data analytics to provide synthetic critical alarms arising from the collation and correlation of multiple lower order alarms.*

3. That Telstra and ESOs (through NECWG-A/NZ) identify procedures and trigger points for reporting and investigation of the reasons for overflow calls (or observed routing difficulties) to ensure that the reasons for overflow are correctly identified and understood by all impacted parties.

4. That the ECP, ESOs and telecommunications carriers investigate capabilities for timely identification and capture of all telephone numbers that have attempted to call Triple Zero during a service disruption, and for the Triple Zero Disruption Protocols to set out the arrangements for those callers to be contacted to ensure their welfare. Call back processes may be undertaken by either the ECP, ESOs, telecommunications carriers or carriage service providers, or a combination of these parties depending on the severity and type of incident experienced.

5. The ECP for Triple Zero should work with DoCA, ESOs and industry to investigate the feasibility of improving network redundancy arrangements, including options for:

   - an optional Session Initiation Protocol (SIP) interface for the direct provision of calls to ECP call centres by telecommunications carriers that prefer to implement and utilise SIP arrangements; and
   - multi-carrier redundancy for the carriage of calls and data from ECP call centres to ESOs (to avoid reliance on a single network for outbound calls).

6. The ECP for Triple Zero should work with DoCA and ESOs on options to provide live dashboard reporting for ESOs that:

   - communicates the status of the ECP network, systems and service provision;
   - identifies and describes any disruptions or service incidents; and
   - provides estimated rectification timeframes.

   DoCA should consider the merits of making live dashboard reporting available to public safety agencies.

7. The ECP for Triple Zero to work with the Triple Zero Coordination Committee to investigate providing alternative contact numbers to facilitate calls to ESOs that can be utilised in the event of a disruption to Triple Zero services. These numbers should only be publicised in the event of a disruption to the Triple Zero service.

8. State and Territory ESOs and their respective government agencies should review their current business continuity and disaster recovery arrangements to ensure there are adequate processes in place to manage incidents within each jurisdiction, including the management of media messaging and communications to the public during a disruption to the Triple Zero service (that is coordinated with the processes set out in the Triple Zero Disruption Protocols).

9. That the ACMA review the *Telecommunications (Emergency Call Service) Determination 2009* to ensure that the Determination:

   - provides adequate protections to the Australian community;
   - takes into account market and technology changes;
   - imposes clear and consistent obligations across the ECS supply chain;

- includes a requirement for timely and effective communication across the ECS supply chain when there is a disruption to emergency services.

As part of the review, the ACMA considers whether any parts of the C536:2011 Emergency Call Service Requirements Industry Code and the G644:2011 Emergency Call Service Requirements Guideline should now be included in the Determination.

10. That the Communications Alliance review the C536:2011 Emergency Call Service Requirements Industry Code and the G644:2011 Emergency Call Service Requirements Guideline (which provides guidance in the event of a DoS attack to the Triple Zero service) to ensure the code and guideline:
    - provide adequate protections to the Australian community;
    - take into account market and technology changes;
    - impose clear and consistent obligations or guidance across the ECS supply chain.
11. The Department of Communications and the Arts should review the terms of reference for the Triple Zero Coordination Committee to ensure the committee has a proactive role in identifying and resolving gaps and risks to end-to-end service delivery for the Triple Zero Emergency Call Service and establish a clear work program to address these.

Introduction

Telstra is the ECP for all Triple Zero calls made in Australia. The Telstra Universal Service Obligation Performance Agreement (TUSOPA) requires Telstra to supply the ECS in accordance with any requirements on the ECP under the TCPSS Act and the related *Telecommunications (Emergency Call Service) Determination 2009* (the ECS Determination).

The ACMA regulates and monitors the provision of the ECS under this legislative framework, which imposes requirements on carriers, carriage service providers and ECPs in relation to the delivery of the ECS. The ECS Determination also includes provisions on prioritising emergency calls and benchmarks for answering emergency calls.

The *Emergency Call Service Requirements Industry Code C5326:2011* mandates network management strategies that are designed to help carriage service providers ensure end users have effective access to Triple Zero.

During the month of May 2018, Telstra experienced two disruptions that affected the ability of individuals to contact Triple Zero. The first disruption (which occurred over 3 & 4 May) occurred over a period of approximately eight hours and resulted in intermittent voice connection interruptions for calls, including to Triple Zero, Australia-wide. The second disruption on 26 May occurred over a period of two hours and impacted calls to the Triple Zero service. The causes of each disruption were distinct.

The process of handling calls to Triple Zero

When a person calls Triple Zero, the call is received by Telstra, the ECP for all Triple Zero calls made in Australia. The caller is first presented to a Recorded Voice Announcement (RVA) advising the caller that they have dialled Triple Zero and will be connected to an operator. The operator then receives the call and asks 'Police, Fire or Ambulance?' and for location details from the caller. The operator then connects the call to the relevant ESO (Police, Fire or Ambulance) in the State or Territory from which the call is being made. Telstra sends to the relevant ESO the Calling Line Identification (phone number), for a fixed line call the address of that service, and for a mobile call, the Push Mobile Location Information

(Push MoLI) data and the registered service address for that mobile service that is provided by mobile carriers for each call.

Where the caller to Triple Zero does not respond at all to the operator, there are no suspicious circumstances associated with the call and there is no indication that assistance is required, there are 'Caller No Response Call' procedures. The ECS Determination requires these calls to be transferred to an announcement for 'Caller No Response Calls'. At this point a message is played three times, prompting the caller to dial 55, and if the caller does not do so the call will be disconnected automatically.

However, where a caller does respond to the operator, but cannot articulate where they are and what they want, such calls are diverted to police. This is because police are considered to be the best equipped of the ESOs to respond to such calls.

The provider of the Triple Zero service is responsible for ensuring that redundancy arrangements are in place to meet its regulatory and contractual obligations. Telstra currently has a dedicated transmission network that prioritises all calls to Triple Zero. The network is designed so emergency calls can avoid any local traffic congestion, with route redundancy provided to allow for alternate dedicated routes if there is a network failure or disruption in a specific location.

Service disruption of 3 & 4 May

Timeline of events[1]

At **03:46** on **3 May** Telstra received an alarm from the 'element manager' of the transmission device at the Exchange One (VIC) identifying that there had been a loss of communication to that transmission device. Telstra describes the failure of the controller card as 'fleeting', indicating the loss of communications was intermittent. The 'loss of communications' meant that no subsequent alarms were presented to Telstra network management staff in the event of any further failure in the transmission equipment, because that equipment was disconnected from the monitoring system. At this time, there was no impact to 000 customer services.

Telstra advised that at the time, this loss of communications alarm was not identified by the Telstra operators. According to Telstra, there were approximately 26,000 alarms present in the alarm system, 13,000 of which were rated as critical. Telstra advised these volumes as being typical in a network of this size.

At **16:55** on **3 May**, Telstra lost its redundant links over Link 1 for the transmission of PSTN services, including 000. There was also a partial loss of transmission capacity for the interstate links over another link (Link 3). At the time, Telstra understood there was no known impact to Triple Zero calls. However, it was later revealed that there was some impact on the routing of calls to ESOs (as seen by the ACT ESOs detailed further below).

At **01:20** on **4 May**, the Melbourne ECP received a call from the ACT Fire Supervisor reporting that they were receiving overflow calls from ACT Police and Ambulance. Telstra understands that this was due to a connectivity issue over Link 3 which resulted in the Melbourne ECP having to make more than one attempt when transferring some calls to ACT ESOs. According to Telstra, ACT ESOs receive overflow calls from the other agencies as part of business as usual processes. Telstra explained in its responses to DoCA of 30 May and 15 August:

[1] Times are in 24-hour format

> *… when transferring calls to an ESO, the ESAP call taker works through a list of alternate contact phone number options for that ESO. In ACT, the options include contact numbers for ESOs other than the one requested. So it is normal for some calls transferred to ACT to be answered by ESOs other than the one requested. In all other States and Territories the list is restricted to contact numbers for the same ESO, e.g. different Police answer points within the same State.… when transferring calls to an ESO, the ESAP call taker works through a list of alternate contact phone number options for that ESO.*

Telstra advised DoCA, on 15 May, that the additional attempts 'may have resulted in calls being presented to alternative ACT ESOs, but the transfers were still successful…'. The ACT Emergency Services Authority advised DoCA of five calls on 3 May 2018, and a further three calls on 4 May 2018 that it understood were routed to alternative ESOs. Telstra's post-incident review has identified 34 calls that required multiple attempts to reach ACT ESOs between 16:55 on 3 May and 00:10 on 4 May.

At **02:05** on **4 May**, Telstra detected multiple Telstra services had failed, including some internal Telstra business systems and applications. Telstra's technical investigations focussed on its IP core network, as this appeared to be the most likely cause of the wider service failure. According to Telstra, these investigations identified that an inter-capital link (Link 2) had failed and was causing network instability within Telstra's IP core network (it was later revealed at 02:42 that the cause was fibre damage near Orange NSW).[2] The fibre failure had a combined effect with other network incidents resulting in:

- the loss of multiple PSTN routes over Link 1 and Link 2, coupled with the loss of redundancy on this route from the fault at Exchange One (VIC) the previous day, caused a major loss of PSTN transmission capacity between Victoria and NSW. This resulted in some Triple Zero calls not progressing through to an operator in the ECP call centres, and some calls having to be manually transferred to ESOs; and
- a high volume of IP routing updates, along with re-routing of IP traffic that, in turn, triggered a previously unknown software fault with some of Telstra's IP core network routers (now known to be a memory leak issue). This impacted the ability of customers to make Triple Zero calls from a range of IP services including mobiles, IP telephony and data services.

At **03:02**, Telstra sent a fibre repair team to the site of the cable cut.

At **03:18**, "memory issues" were identified in the IP core network routers located in Exchange Two (VIC) and Exchange Three (NSW).

At **03:31**, the impacted core routers at three other Telstra exchanges were isolated, allowing restoration of Telstra IP-based services to commence at 03:40.

At **05:33**, a similar issue was identified by Telstra in an IP core network router located at Exchange Five (QLD) (with an impact on calls to emergency services), and the router was isolated.

At **07:30**, Telstra identified the potential significance of the Link 1 transmission controller card failure that commenced on 3 May. Actions were initiated to replace the controller card, which was suspected of preventing Link 1 from carrying PSTN traffic inbound from NSW, the ACT and Queensland to the Melbourne Triple Zero call centre, and outbound to NSW, the ACT and Queensland from the Melbourne Triple Zero call centre.

Between **08:32** and **08:55** Telstra experienced another incident in its core IP network. A router in Exchange Four (NSW) encountered a memory-related issue similar to that which had impacted core

[2] An investigation into the cause of the fire was conducted by the NSW Rural Fire Service. The investigation was finalised on 30 May 2018 and concluded that the cause of fire was undetermined.

routers at the three other exchanges (although in this case unrelated to the impact on the IP core network, which flowed from the Orange fibre damage). This impacted a number of IP services, including some mobile and Telstra IP Telephony (TIPT) services. The router at Exchange Four (NSW) self-recovered with impacted services restored without any manual intervention.

At **10:38**, repair of the damaged fibre cable at Orange was completed. This restored the majority of the impacted PSTN services, including the calls to the Triple Zero service, to normal operation. However, there were residual connectivity issues between the Triple Zero call centre in Melbourne and ACT ESOs, which meant that Melbourne ECP operators were still having to make more than one attempt to transfer some calls to ACT ESOs.

By **12.10**, the redundancy for PSTN and the Triple Zero call routing between Victoria and NSW was restored, coinciding with the completion of the repair of the faulty controller card for the transmission device for Link 1. This also resolved the residual connectivity issues between the Triple Zero call centre in Melbourne and ACT ESOs.

Impact on Triple Zero calls

The result of the outage was that some Triple Zero calls did not progress through to an operator in the ECP call centres, and some calls had to be manually transferred to ESOs. In some circumstances where calls were unable to be transferred to an ESO using standard methods, the details of the caller to Triple Zero were provided to supervisors in Telstra call centres and subsequently relayed to supervisors within ESOs through dialling alternative phone numbers (such as the supervisor's contact number).

Telstra submitted in its response to DoCA dated 15 May that:

> *For callers who were able to make outbound voice calls, the transmission network successfully delivered triple zero calls to the Emergency 000 platform, which is comprised of the 000 exchange switches, along with the network routing between them, and to the ESAP agents. However, due to the severing of the Victoria to NSW links some functionality across the four redundant 000 handling switches was impacted meaning some calls were unable to be delivered to the operators, and some calls were unable to be transferred automatically to ESOs, on opposite sides of the interstate failure between NSW and Victoria.*
>
> *This is because there are two dedicated 000 ESAPs, one in Sydney and one in Melbourne. The 000 service is configured to automatically direct calls to the centres in Sydney and Melbourne based on the location of the caller and wherever the next available operator is located. Due to the geographic nature of the PSTN impact, if a 000 caller in NSW, the ACT or Queensland was automatically routed to the Melbourne ESAP centre then that call may not get through. Similarly, if a call from Victoria, South Australia, Western Australia, Tasmania and NT was automatically routed to the Sydney ESAP call centre it may not get through. That is why some people needed to redial 000 one or more times to make a successful connection, or may have chosen to use other means such as trying an alternate line or seeking other means of assistance.*

There were four categories of calls to Triple Zero that were affected:

1. Calls made to Triple Zero that did not reach the Recorded Voice Announcement (RVA)
2. Calls that did reach the RVA but did not reach an operator (they were disconnected after receiving an Interactive Voice Recording)
3. Calls that were connected to the operator, but that required multiple attempts of transfer or manual intervention in order to reach the ESO

4. Calls that were rerouted from one ESO to another ESO to manage congestion and routing issues (due to multiple or delayed transfers, or manual transfers).

Under 'overflow' arrangements agreed between each State/Territory and Telstra, some calls were directed to alternative ESOs in some States/Territories and then details of the calls were provided to the correct ESO through either ICEMS/Inter-CAD arrangements, or other procedures for relaying details between ESOs.[3]

Some individuals may have needed to attempt to call Triple Zero several times before successfully connecting to an operator.

Telstra provided data (for the period from 02:05 to 10:38 on 4 May) identifying the number of callers on the basis of unique A-Party caller outcomes, and on a call outcome basis. On a unique A-party basis there were:

- **6,898** unique A-Party callers;
- **2,081** callers hung up during the RVA greeting;
- A further **869** callers did not connect to a Telstra Triple Zero operator (**322** callers hung up while waiting for the operator and **547** callers received a congestion tone or message after the RVA);
- **3,948** callers reached a Triple Zero operator (some of these would have required several call attempts to reach an operator). Of those, **3008** genuinely required an ESO[4]. All **3008** callers were successfully connected to an ESO (**2882** on a single attempt and **126** after multiple attempts).

On a call outcomes basis (total number of calls to Triple Zero) there were:

- **12,224** calls;
- **3,182** calls hung up during the RVA greeting;
- A further **3,894** calls did not connect to a Telstra Triple Zero operator (**1,438** callers hung up while waiting for the operator, and **2,456** received a congestion tone or message after the RVA);
- **5,148** calls reached a Triple Zero operator. Of those, **3,739** genuinely required an ESO. All **3,739** calls were successfully connected to an ESO (**3,472** on a single attempt, and **267** after multiple attempts).

All callers that connected to a Triple Zero operator were successfully handed to an ESO either:

- via normal transfer; or
- via manual processes whereby an agent would write a ticket and advise the caller they would pass on their phone details for the ESO to call them back. These tickets were then called through by a supervisor in each Telstra call centre to supervisors at ESOs.

Callers affected by the Outage

Of critical importance among any findings is the wellbeing of any caller that could not get through to the Triple Zero service or who experience significant delays in being transferred to the appropriate ESO.

[3] ICEMS and Inter-CAD are electronic messaging systems that provide incident requests between ESOs (for example a Police service requesting an Ambulance service provide assistance at a car crash).
[4] Callers not required to connect to ESOs were misdials, test calls, nuisance calls or hang ups.

For example, an incident[5] was reported in Redfern NSW where a resident of a house was unable to reach the ECP and consequently drove to the closest Fire Station to raise the alert about a fire started by an electric blanket in the home.

Telstra conducted welfare checks on callers who could not get through to Triple Zero. Telstra reached out directly to all those people it was aware of, such as those involved in the Redfern example above, who may have been impacted by the incident.

DoCA recognises, that there may be individuals impacted by the service outage that have not been brought to DoCA's attention at this time.

Procedures for Managing Triple Zero Disruptions

Procedurally, Telstra has in place a number of Incident Management Processes, Work Instructions, Business Continuity Plans and other documented Standard Operating Procedures.

In its investigation report provided to DoCA on 15 May, Telstra advised the following procedural documents (among others) were invoked on 3 & 4 May:

1. Emergency Service Answer Point (ESAP) – Business Continuity Plan (BCP); and
2. Disaster Recovery Manual for the Triple Zero (000) Call Centres (DRM).

Telstra advised that these are the two relevant procedural documents for incidents specifically related to the ESAP. These documents contain Telstra's processes for dealing with operational events (including unplanned events) that could cause disruption to the ECS. Telstra stated that the purpose of the BCP 'is to capture workaround strategies that can be invoked by the ESAP call centres to continue the handling and transferring of Triple Zero calls in the event of a disruption'.

Separate to the BCP and DRM, Telstra has processes in place from its standard Incident Management process framework. These are applicable to identifying and repairing an outage on an inter-capital transmission link, such as the NSW-Victoria links, and provide an outline of a range of timeframes and operational steps depending on the nature and severity of an incident. They include:

- Incident Management Process and Work Instruction
- Incident Management, Telstra Service Operations
- Major Incident Management process

In response to DoCA's request for details about what, if any, operational procedures it has in place for managing an outage of the magnitude of the 3 & 4 May Outage, Telstra advised that, during major incidents, it invokes its Crisis Management Team (CMT) and its Major Incident Management (MIM) processes. This was done on 4 May. In its response to DoCA of 30 May, Telstra stated:

> *The role of the CMT is to control and minimise loss (human, customer, operational, financial, environmental and reputational) related to an escalating serious incident or crisis, and to protect the interests of all the stakeholders associated with the business. The CMT comprises senior managers from across Telstra, who are called together via an audio/video conference bridge to oversee the resolution of the incident. The MIM team is responsible for driving resolution of high severity incidents relating to networks and technology. This includes coordinating with internal*

[5] Telstra reported this incident to DoCA on 4 May and provided an update on 27 June 2018. The incident was also reported in the Media both on and in the days following 4 May)

> *operation teams and management to resolve the incident. Both CMT and MIM team were engaged on 4 May.*

The Incident Management Process and Work Instruction contains the basic steps for effective incident management including: incident detection and recording; investigation and diagnosis; restoration, resolution and recovery; and incident closures.[6] Incident detection and recording captures detection by alarms, service monitoring and customer reported faults or social media.

The Incident Management Process and Work Instruction includes a 'Communication Process'. It states 'Communications and Notification team submit notification to internal & external stakeholders as required' and adds that this is 'ongoing throughout incident lifecycle'.

In response to DoCA's query about stakeholder communication protocols in place for such outages, Telstra advised on 30 May:

> *Communication protocols are in place for such outages, and the protocols are known to the ESOs. For example, a Fault Reporting Procedure about what to do in the event of a fault with the transfer of calls to them, is sent out to ESOs as a reminder on an annual basis and discussed as required by ESOs. Another example is Section 9.10 of our Emergency Call Person [support] Policy 0003750 … which sets out the procedures to be followed in the event that there are problems in transferring a call from the ESAP to an ESO.*

Telstra provided the relevant Emergency Call Person Support Policy. It is noted that section 9.10 states:

> ***Delay in ESO answering***
>
> *If the ECP has problems connected (sic) to a call to an ESO, i.e. frequently rotates through choices in priority for the same ESO without success, the Team Manager must be notified. There are occasions when an undetected problem may exist and the Team Manager may be required to contact the ESO to advise them of this. Each Call Centre has a current list of contact numbers for each State ESO. These numbers should only be used by the Team Manager if agents are having problems connecting a call to an ESO.*

Regarding its internal communication processes, Telstra advised that network incidents are communicated to its staff through a number of platforms and channels, depending on the part of the organisation in which they work. Its communication system for internal distribution of notifications about outages is via email and text messages. It also advised that Telstra employees can self-subscribe to the notifications in accordance with the technology and severity type categories they wish to be informed about.

Adequacy of Procedures and Response

Initial identification of network problems

Telstra's network alarm system identified there had been a 'loss of communications' (for the transmission device in Exchange One (VIC)) to the network monitoring system at **03:46** on 3 May. The 'loss of communications' alarm was activated but not identified by Telstra staff among 26,000 alarms present in the system at the time. This 'loss of communications' meant that no other subsequent alarms would be presented to Telstra staff in the event of any further failure in transmission equipment in the Exchange One (VIC) network device because that equipment was disconnected from the monitoring system.

[6] *Service Assurance Operations, Incident Management Process & work Instruction*, pg. 4

At **17:38** on 3 May Telstra raised an internal ticket for the 'loss of redundant signalling' alarm to be repaired on the next business day. Telstra's response to DoCA indicates that Telstra only identified the importance of the 'loss of redundant signalling' at around 07.30 on 4 May, when Telstra technicians were mobilised to attend the relevant exchange and make repairs.

It is evident that neither ECP call centre operators, ECP's Team Manager on duty at the time, nor Telstra's systems identified the pattern of calls unsuccessfully routing to correct ESOs in the ACT on the evening of 3 May 2018. DoCA acknowledges Telstra's submission that 'it is not uncommon for a Telstra call taker to work through at least the first few choices on the re-selection tree'. When the ACT Emergency Services Agency raised these issues with Telstra, Telstra conducted a test call, but this did not identify any problem with transferring calls to ACT. Despite this action being taken, DoCA observes that Telstra's processes for escalation when a call operator encounters certain patterns of overflow calls could be improved to provide more clarity when a call operator should escalate such situations to a Team Manager for investigation.

Telstra has advised that the vendor root cause investigation into the failure of the network device in Exchange One (VIC) identified three separate faults:

1. a hardware fault that only impacted internal and external card communications, but did not have any direct impact on the traffic handling capacity of the device;
2. a data communication fault between two switching modules and an interface card which impacted the traffic handling and redundant traffic switching capability of the device. This resulted in some traffic failure on the circuits between Melbourne-Sydney and Melbourne-Canberra, including some Triple Zero traffic to Canberra ESOs; and
3. a faulty data card which had no impact on traffic as it had no active services. However, fleeting alarms from this card resulted in logs being overwritten which has impacted post event root cause investigations.

Business Continuity Plan

DoCA's review of Telstra's BCP for the ESAP identified the document was last updated in October 2016. In DoCA's view there are deficiencies in the BCP with respect to communication with stakeholders. Other than saying 'communicate to stakeholders' internally and externally, they do not identify how Telstra will communicate with stakeholders if any of the events in the BCP do occur.

The BCP lists external stakeholder contacts, including relevant names and telephone numbers, in addition to specific contact numbers to reach each ESO call centre. DoCA identified six ESO management contacts incorrectly listed, as the listed contacts no longer held these positons, either on a permanent basis or due to secondment to other agencies or positions at the time of the outage. It is further noted that three ESOs had no management contact listed, and that the Emergency Services Telecommunications Authority (ESTA[7]) (Vic) was not listed as a stakeholder. The BCP stakeholder list also does not list any email addresses for external stakeholders, meaning that there was no form of mass communication prepared or available to send out information to one or more ESOs during the incident.

Given that most scenarios in the BCP require one or more ESOs (or commonly all ESOs) to be contacted regarding an adverse event, the BCP is deficient as it does not set out the relevant contact details or processes necessary to reach relevant stakeholders. Telstra later advised DoCA that separate contact lists are used for notifications to ESOs which include email addresses and mobile phone contacts.

[7] ESTA is vested with responsibility for the provision of multi-agency emergency services communications across Victoria, including all Triple Zero call-taking and the dispatch of police, fire and ambulance emergency services.

However DoCA notes that the lack of any information in the BCP to indicate these alternative contact lists exist, or where they can be accessed if needed, points to deficiencies in the BCP.

While a number of the scenarios in the BCP identify that ESOs should be notified of an adverse event using the stakeholder contact list, DoCA considers that timeframes for notification of ESOs should be considered during development of the Triple Zero Disruption Protocols. Current timeframes specified in the BCP are as low as 10 minutes for some scenarios, and commonly 20 minutes for most scenarios. Given that calls to Triple Zero and ESOs may already be impacted, DOCA considers that the earlier advice can be provided to stakeholders the sooner back up plans can be implemented at the State/Territory level for successful mitigation of any detrimental impacts. Feedback from ESOs is that they should be aware of any adverse event (even events not understood to be directly impacting their own service) to ensure they have full awareness of the operating environment. This will also assist ESOs to identify and diagnose any problems impacting their own services at the same time that may be related, or unrelated to the pre-existing event.

Telstra's Internal Communication

During the outage, ESOs and other stakeholders, unable to obtain information from Telstra by contacting the Telstra ECP or its management, attempted to obtain information from other contacts within Telstra (including through account managers for their telecommunications services). It is evident that Telstra's internal staff were not necessarily informed of the reasons for the outage, or the impact on Triple Zero services, and were unable to provide reliable information to stakeholders. This may have been due to the complexity of the service outage, with multiple impacts on Telstra's network making it difficult to diagnose and communicate causes, when they were actively being managed over the duration of the outage.

Problems with Telstra's network compounded internal communication problems by making it difficult for internal communication platforms to communicate messages, and to contact staff and receive regular updates about remediation activities. For example as the TIPT product was not operating at times, relevant staff were unable to dial into the MIM teleconference bridge to assist in diagnosis of the problem. Telstra submitted to DoCA:

> *From 2.05 am there was a loss of connectivity to the internal communication system which prevented initial advice being distributed. Connectivity to the internal communication system was progressively re-established commencing at 2.42 am, from which time, notifications were intermittently sent from the internal communications system to subscribed staff followed by subsequent progress updates.*
>
> *As there were a number of individual network events which contributed to the disruption of services, we were undertaking investigative and remedial action as events unfolded. This meant that there were times when we thought services had been restored only to learn that some calls were still failing. This may have led at times to Telstra staff providing incorrect information.*

Telstra's internal fault reporting lines were also unable to accept fault reports immediately after Link 2 was disabled, and Telstra's ECP fault management staff advised that faults would not be able to be logged for 30 minutes due to IT problems. This appears to have delayed effective resolution of the outage.

The fibre repair crew dispatched to the site of the fibre-optic cut near Orange in NSW, was also hampered by a lack of communications connectivity. As the repair location was outside Telstra's mobile coverage, the repair crew was reliant on a satellite phone for communications. However due to a fault, the satellite phone was only able to receive calls, and staff were not able to make calls (Telstra report 27 July 2018). Telstra has advised the Department that this did not impact the ability of the repair crew to fix the fibre-optic cable. Telstra has subsequently purchased 37 new satellite phones for repair crews.

Communication with stakeholders

A critical component to the management and restoration of the 3 & 4 May Outage was the communication of each event with relevant stakeholders as they unfolded. DoCA has already noted above its observations on the adequacy of the BCP with respect to communications with stakeholders and Telstra's internal communications.

According to Telstra's advice on 15 May, it took steps to inform key government stakeholders, other carriers and the media. Telstra noted that on 4 May, it initiated contact with:

- DoCA at 07:48 (noting DoCA attempted to contact Telstra at 07:28, when it became aware of media reports);
- the ACMA at 08:22;
- the Federal Government, Communications Minister's office at 08:39;
- State and Territory Premiers 'in the afternoon' of 4 May;
- State and Territory Ministers, Commissioners and Departments 'from the morning' of 4 May;
- Telstra Wholesale customers initial notification at 03:02 on 4 May;
- Media statements were issued at progressive intervals, commencing at 05:38 on 4 May.

Regarding communications with ESOs, Telstra advised that for the duration of the outage, it was contacting ESOs that, at that time, Telstra believed were impacted, in order to triage the incident and advise them about the incident. It submitted that, on the day of the 4 May outage, both its BCP and DRM were invoked, and that:

> *[t]his resulted in a number of interactions being initiated in both directions between the ESAP and the ESOs as well as between the ESAP and Telstra's internal incident management teams. Telstra initiated calls to those ESOs which, to the best of its knowledge at that time, were impacted. Telstra also received calls from various ESOs and gathered information on the scope and symptoms of the disruption, which helped identify and diagnose possible causes. Telstra also communicated with ESOs, both at an operational level to ESOs, and later in the morning, Telstra executives engaged with relevant agency staff.*

DoCA received some contradicting accounts with respect to who contacted whom and on how many occasions throughout the outage. The majority of ESOs however consider Telstra's communication with stakeholders was inadequate, and that Telstra was unprepared for the events that occurred on 3 & 4 May.

ESO submissions

DoCA wrote to ESOs on 8 May, and met with ESOs in two meetings held on 14 and 15 May. DoCA sought information regarding the ESOs experience with the impact that the outage had on their ability to receive calls; communications received from Telstra during the outage; details about any unsuccessful calls to Triple Zero, and details of inquiries into the safety and wellbeing of anyone who attempted to make those calls.

In addition to the input provided at the 14 and 15 May meetings, written responses were received between 11 May and 5 June. A majority of the ESOs expressed concern with the frequency and type of communication received from Telstra throughout the incident. Some advised that they received no contact from Telstra at all, both during and after the event, and that they were informed of the outage via other ESOs or the media. Most of the ESOs were required to initiate contact with the Telstra ECP to advise they were experiencing issues.

For example, one advised:

> *[Agency] has on no occasion received any notification, update or communication from Telstra related to the Triple Zero (000) Emergency Call Service Outage either during or post the incident. This includes communication notifying [Agency] that the outage was occurring, had occurred, the reason for the outage or any communication as to the resolution.*

Others advised that they experienced difficulty contacting Telstra once the ESO detected issues to the service, for example:

> *There were difficulties in our ability to contact Telstra from our technical team on the corporate reporting number. [Agency] technical team were placed in a queue with an automated voice recording on hold for approx. 15 minutes and then disconnected on several occasions with the same result. [Agency] reverted to an SMS at 2.35 am to the [State] based Telstra Service Delivery Manager (SDM) again with no immediate response.*

Some advised that where contact was received, the unprecedented nature of the event meant information provided was inaccurate or inconsistent with media reports:

> *The event experienced by Telstra was unprecedented and unforeseen. The combination of these factors contributed to errors in the management of the incident on this occasion. Consequently, the frequency of updates provided by Telstra did not meet the needs of the [Agency] and real-time information was not forthcoming during the event.*
>
> *The information relating to the network's restoration was inaccurate and this inaccuracy resulted in the [Agency] and Telstra providing contradictory public messaging.*

In its response to DoCA on 17 May, an ESO expressed concern with Telstra's management of the outage, particularly its 'failure to communicate, consult, or assist in supporting the [State's] Triple Zero service in any meaningful way throughout the incident and since.'

One of the ESOs stated that it was not clear whether Telstra had complete visibility of the cause of the issues, or if they were simply reluctant to advise what the issue was. There was apparently confusion throughout the morning where information had been received from Telstra that their systems were restored, however, the ESOs own systems were demonstrating otherwise.

ESOs have raised concerns with DoCA that, after the incident, they have operated without a full understanding of the number of callers that tried to reach them on 3 & 4 May, and the number of calls that may have been handled by an alternative ESO within their State/Territory, or handed to an ESO in another State/Territory (a number of calls are known to have been handled by ESOs in a different State/Territory and subsequently passed back to a relevant ESO in the correct State/Territory for response). This is best described by ESOs using the phrase "we don't know what we don't know".

A number of ESOs advised that they were not contacted by Telstra for an update on the calls that may have tried to call Triple Zero and did not reach a Triple Zero operator due to failures within Telstra's network. It is evident that Telstra has experienced difficulties in quickly acquiring this data from its systems, and this led to significant delays in the provision of this data or failure to provide this data to ESOs. In some circumstances where data has been provided, further additional data sets have been provided after Telstra's continued investigation of the incident.

Telecommunications carrier submissions

DoCA also sought information from the major telecommunication companies regarding their experience with Telstra during the outage and follow up on welfare checks for calls that were made to Triple Zero. Similarly to the ESOs, there was a high level of frustration about the level of communication from

Telstra throughout and following the incident. One telecommunication company advised that Telstra did not acknowledge or proactively communicate that there was an issue until 08:01, which was nearly six hours after its Technology Operations team first observed Triple Zero call failures and specifically raised the issue with Telstra.

This is consistent with Telstra's account of communication with CSPs and carriers. Telstra stated on 30 May:

> *As part of our communication to wholesale customers, a number of major carriers were provided with an automated email notification at 3.02am advising them of the outage in Orange and providing them a list of all their potentially impacted data services. There was no reference to Triple Zero in this initial communication.*
>
> *Just after 8.30, we updated the Customer Portal for our wholesale customers that this outage was ongoing and it included impact to Triple Zero. This is available to all wholesale customers. Conversations were held with the major carriers including updates later in the morning. Post event, some key carriers were provided with a Customer Impact Statement providing more details of the event.*

A telecommunications company also wrote to Telstra seeking cooperation in quickly developing a joint crisis management plan for substantial and high profile incidents such as that experienced on 4 May. Concern was also expressed that redundancy measures were not properly in place, tested and working and that there was little communication from Telstra relative to the seriousness of the issue.

Actions taken

In response to the incident, Telstra identified and repaired the immediate causes of the 3&4 May Outage, which included the damaged fibre cable and the faulty transmission hardware in Exchange One (VIC) (impacting Link 1).

Telstra has conducted its own investigation of the incident and identified a number of improvements to policies and operational practice that will be implemented to help prevent similar disruptions occurring, or to more effectively manage a disruption should it occur. These include improvements in the following categories:

- **Network redundancy** – including the provision of additional redundancy between Victoria and New South Wales, on other major transmission routes, and ongoing review of appropriate options on other transmission routes.
- **Network alarming** – including deployment of a more advanced alarming system, with improved root cause determination capabilities, topology awareness, service impact determination and enhanced alarm enrichment capabilities. DoCA notes that Telstra has already
    - improved the visibility of 'Loss of Communications' alarms within its network
    - automated tickets of work to initiate incident restoration activities for loss of communication events;
    - implemented alarm collection system improvements to allow correlation of alarms to parent alarms;
    - refining of alarms to provide improved visibility for operators; and
    - implemented big data analytics initiatives to provide synthetic critical alarms arising from the collation and correlation of multiple lower order alarms.
- **IP router remediation** – including working with router vendors to have patches implemented in routers (patches installed between 17 May and 6 June), and a new platform toolset to allow improved monitoring of router in Telstra's IP network.

- **Vendor management** – amended contractual arrangements between Telstra and equipment vendors, and additional vendor support for issue troubleshooting.
- **Incident management**
  - improvements to, and clarification of the roles and responsibilities of Telstra's CMT vis-à-vis other internal stakeholders involved in management and investigation of an incident, and clarity to the role of reviewing and approving internal and external stakeholder communications;
  - improved communication plans for the emergency call sector and the public.
- **External and Internal Communications**
  - working with the NECWG-A/NZ , telecommunications carriers and CSPs to understand the impact of the outage;
  - development of a teleconference bridge to discuss and provide regular updates to ESOs during any disruption to Triple Zero services;
  - development of Triple Zero Disruption Protocols based on NECWG-A/NZ's draft Triple Zero Disruption Protocols (NECWG protocols to be finalised mid-August 2018 and Telstra protocols in September 2018); and
  - development and execution of end-to-end service disruption simulation exercises to test and optimise improvements.
- **Benchmarking** – Telstra is conducting a benchmarking exercise with network operators across the globe who have similar network architectures and emergency calling obligations to ensure Telstra is utilising world's best practice in architecture and resiliency.

DoCA acknowledges that the response to the disruptions and the improvement process is ongoing.

NECWG-A/NZ Actions

NECWG-A/NZ discussed the outage at its meeting on 23 May 2018. NECWG has produced a draft "Triple Zero Disruption Protocol Recommendations" document which has been provided to ESOs for comment. This document was finalised in mid-August 2018 and will inform work by DoCA and Telstra to develop and agree protocols for managing any future outages.

Triple Zero Coordination Committee (TZCC) Actions

The NECWG-A/NZ document and the Triple Zero Disruption Protocols were discussed at the Triple Zero Coordination Committee (TZCC) meeting (chaired by DoCA) on 6 July 2018. TZCC members agreed to a work plan for the development of the Triple Zero Disruption Protocols which will involve:

- Telstra leading drafting of the Protocols (given its role as ECP), based on the NECWG-A/NZ Triple Zero Disruption Protocol recommendations;
- Telstra consulting with ESOs, telecommunications carriers and government stakeholders during drafting and development of the plan.

ACMA Investigation

Section 147(1) of the TCPSS Act requires the ACMA to make a determination imposing requirements on carriers, carriage service providers, and emergency call persons in relation to emergency call services. The ACMA monitors and enforces compliance with the ECS Determination. The ACMA is conducting an investigation under section 510 of the Telco Act into the Triple Zero Outage and has sought information

from Telstra under section 521(2) of the Telco Act. The investigation is assessing Telstra's obligations both as ECP and also as a carriage service provider and carrier under the ECS Determination and the *Emergency Call Service Requirements Industry Code C5326:2011*.

The ACMA's investigation into Telstra's compliance under the regulatory framework is underway.

26 May Incident

On 26 May, Telstra experienced another disruption to its Triple Zero Service, however, on this occasion the circumstances were different to the 3 & 4 May disruption.

Specifically, on 26 May on three occasions between 06:09 and 08:01, Telstra's 000 operators received a series of approximately 600 calls – two bursts within 60 seconds and one period across 35 minutes. These calls came from multiple numbers and were answered by operators and consistent with protocol, directed to the Caller No Response – Interactive Voice Response (CNR-IVR) system which asks the caller to press '55' if they require assistance. In some cases, repeat calls were directed to police in the State in which they were determined to have originated.

Telstra advised DoCA that some of the non-verbal calls were able to pass through the CNR-IVR process to be connected to Police due to them being falsely treated as 'return 55' calls by Telstra's system. Other calls were presented to Police as a result of the incoming Triple Zero call queues being busy which forced calls to overflow to Police.

Telstra treated this as a DOS incident in accordance with the relevant *Communications Alliance Emergency Call Services Requirements Guideline G644:2011.* The Guideline contains processes for management of Denial of Service incidents, which supplements the *Emergency Call Service Requirements Code C536:2011*.

DoCA has reviewed the procedures undertaken by Telstra during the incident and found all procedures to be consistent with the Guideline. Telstra has undertaken a number of actions to deal with DoS incidents, including implementation of enhanced monitoring tools which will assist in identification of DoS incidents, heightened monitoring and mitigation strategies, and tools to block calls from third-party networks if necessary.

Cause of disruption

The calls were from an IP-based subsidiary service of iPrimus, owned by Vocus.

Vocus advised Telstra on 31 May that the cause was an attempted international toll fraud on one of its customers. These calls were unintentionally routed to the Triple Zero call centres. Vocus advised it has taken steps to prevent this type of attack from reoccurring.

Impact on Triple Zero Calls

Telstra initially advised that the incident affected call response times, but the network was otherwise functioning as normal. There were, however, a number of genuine callers who were unable to successfully connect to a Triple Zero operator due to congestion of lines into the Triple Zero call centres. Subsequent analysis of the calls during the relevant period identified:

- a total of 158 potentially genuine callers who reached the operator but were unable to be answered (that is, callers that decided to hang up while waiting in the queue); and
- 10 of the callers made calls from payphones.

Telstra first commenced making call backs to these customers to verify their welfare at 16:47 on 26 May. This was when it completed the analysis of the initial tranche of call data to identify any Telstra callers that were unable to be successfully connected to a Triple Zero operator.

At 18:40, Telstra completed its analysis of additional call data to identify any callers from other carriers that were unable to be successfully connected to a 000 operator. At this time, Telstra commenced making call backs to these customers to verify their welfare.

Between 17:45 and 20:23, Telstra contacted other carriers (Vodafone, Optus, AAPT, Soul Pattinson, Primus, and Lyca Mobile) to inform them about the impact on 000 calls from their networks and advised that Telstra was conducting call backs to check the welfare of the callers. Vodafone elected to make its own welfare checks (for 23 callers).

On 27 May, Telstra advised it conducted all call backs of potentially impacted callers (some were transferred to RVA messages).

On 28 May, Telstra followed up on further calls to the numbers that had transferred to voice-mail messages during the call backs.

The telephone numbers of 21 potentially impacted callers who could not be contacted were referred to Police for follow up.

Telstra advised that it did not identify any negative health or safety outcomes due to callers not having their Triple Zero calls answered.

Communication with stakeholders

According to Telstra, all Federal and State government stakeholders, including the Minister's Office and DoCA, were notified either by phone or email, by midday 26 May.

Telstra first alerted ESOs at 08:32 and provided subsequent updates at 09:48, 10:30 and 11:30 (at which time it advised that no further unusual activity had occurred since 08:00).

There have been no reports from ESOs that they were not properly advised of the incident and DoCA considers this to be a marked improvement to the communication from the 3 & 4 May Outage.

However, in a letter from a telecommunications company to Telstra dated 1 June, the company expressed concern that there was again a failure in communication by Telstra in relation to this incident. The company stated:

> *Since the failure was beyond [its] point of interconnect with Telstra, this issue was not apparent to [the company] and there was no way we could have become aware of the failures without communication from Telstra. The [company] team was only made aware of the issue after a brief and informal phone call at 5.50 pm, with the formal communication regarding the issue being received at 7.03 pm – some 13 hours after the issue was initially apparent to Telstra.*

DoCA considers that it took Telstra too long to advise telecommunications carriers of the incident. Carriers are integral to the Triple Zero service delivery, and need to be made aware of failures as they may assist in speeding up the diagnosis and rectification of the issue. It would not take any significant change in the processes used on the day for carriers and carriage service providers to be contacted at the same time as ESOs, as it would simply require including them on the bulk ESO email list.

Overall, it is evident that some of the observations and subsequent recommendations about communication during the 3 & 4 May incident equally apply to apply to the 26 May incident.

Findings and Recommendations: 4 May and 26 May Incidents

The emergency service environment in Australia is complex, with responsibility for delivery of an end-to-end service carried by the Australian Government, State/Territory Government's (including their ESOs, PSAs and other departments/agencies), and telecommunications carriers and carriage service providers. Telstra holds a unique position in the system as it is a carrier/carriage service provider delivering calls to the ECP, as well as being the ECP, and it is the carrier delivering calls to ESOs (in its role as ECP). This complexity presents unique challenges for the diagnosis of service delivery issues, and communication around those issues to hundreds of staff external to Telstra with responsibility and interest in successful delivery of all Triple Zero calls.

These disruptions to the Triple Zero Emergency Call Service are the first known disruptions since the Commonwealth entered into contractual arrangements in 2012. Under the TUSOPA, Telstra is required to meet a number of regulatory benchmarks related to the delivery of the service. Since the commencement of the TUSOPA, Telstra has met all of these benchmarks, indicating that the service has been reliably delivered for a considerable period of time. DoCA recognises that the historical performance of the service has been high, while noting that the recent events require additional processes and protections to ensure the service continues to meet the high expectations of the Australian community.

DoCA received consistent feedback from ESOs and carriers that the level of communications, and the quality of communications, were deficient on 3 and 4 May, with improvements made by 26 May. Improved communication is required from the ECP to ensure that ESOs, public safety agencies, telecommunications carriers and carriage service providers are:

- always aware of the status of the Triple Zero service;
- informed about any incidents, the severity of incidents, and the estimated rectification timeframes (even if that incident does not directly impact that stakeholder);
- able to implement their own back up plans or action plans to minimise any disruption or risk to callers to Triple Zero; and
- able to ensure improved and consistent communication to the public about any disruption to services, and advise the public how they can contact emergency services during this time.

Recommendation 1

That communications from the Emergency Call Person (ECP) to Emergency Service Organisations (ESOs), public safety agencies, telecommunications carriers, carriage service providers, media, other government stakeholders and Ministers are improved through the development of Triple Zero Disruption Protocols. Development of these protocols should be led by the ECP, and approved by members of NECWG-A/NZ and the Department of Communications and the Arts (DoCA) Triple Zero Coordination Committee.

The early identification of potential loss of redundancy within the telecommunications network used by the ECP, and improved identification of the importance of specific alarms within the network may have helped prevent or minimise the outage of 4 May 2018.

Recommendation 2

That Telstra finalise its review of its network alarm systems and take action to ensure that "loss of communications" alarms are actively identified for rectification.

Note: Telstra has already implemented the following actions to meet this recommendation:

- automated tickets of work to initiate incident restoration activities;
- implemented alarm collection system improvements to allow correlation of alarms to parent alarms, and refining of alarms to provide improved visibility for network managers; and
- utilising big data analytics to provide synthetic critical alarms arising from the collation and correlation of multiple lower order alarms.

There were indications that problems existed within Telstra's network on 3 May, when calls 'overflowed' to alternative ESOs in the ACT. While these call routing problems were identified by ACT ESO staff, and discussed with Telstra, there are presently no clear guidelines or procedures for ESO staff or Telstra staff to trigger fault reporting and further investigation in this specific scenario.

Recommendation 3

That Telstra and ESOs (through NECWG-A/NZ) identify procedures and trigger points for reporting and investigation of the reasons for overflow calls (or observed routing difficulties) to ensure that the reasons for overflow are correctly identified and understood by all impacted parties.

Telecommunications carriers and ESOs provided feedback that the collation of call data to identify callers to Triple Zero that may not have reached a Telstra operator was too slow given the importance of the ECS to save lives. Improvements to these arrangements should be implemented by the ECP, ESOs and telecommunications carriers and carriage service providers.

Recommendation 4

That the ECP, ESOs and telecommunications carriers investigate capabilities for timely identification and capture of all telephone numbers that have attempted to call Triple Zero during a service disruption, and for the Triple Zero Disruption Protocols to set out the arrangements for those callers to be contacted to ensure their welfare. Call back processes may be undertaken by either the ECP, ESOs, telecommunications carriers or carriage service providers, or a combination of these parties depending on the severity and type of incident experienced.

The existing Triple Zero service relies on the network of a single carrier to ensure the carriage of calls from all other carriers and carriage service providers successfully reach a Triple Zero call centre, and can subsequently be transferred to an ESO for response. Reliance on a single network exposes the Triple Zero service to an unnecessary level of risk that could be better managed through multi-carrier redundancy arrangements.

Recommendation 5

The ECP for Triple Zero should work with DoCA, ESOs and industry to investigate the feasibility of improving network redundancy arrangements, including options for:

- ***an optional Session Initiation Protocol (SIP) interface for the direct provision of calls to ECP call centres by telecommunications carriers that prefer to implement and utilise SIP arrangements; and***
- ***multi-carrier redundancy for the carriage of calls and data from ECP call centres to ESOs (to avoid reliance on a single network for outbound calls).***

Given the extensive number of stakeholders that have a significant interest in the successful operation of the Triple Zero service, communication of service disruptions requires a one-to-many solution that does not require verbal updates to be provided to a large number of stakeholders. The draft NECWG-A/NZ Triple Zero Disruption Protocols note the need for a website to support coordinated and consistent communications and a single source of truth.

Recommendation 6

The ECP for Triple Zero should work with DoCA and ESOs on options to provide live dashboard reporting for ESOs that:

- ***communicates the status of the ECP network, systems and service provision;***
- ***identifies and describes any disruptions or service incidents; and***
- ***provides estimated rectification timeframes.***

DoCA should consider the merits of making live dashboard reporting available to public safety agencies.

During the 4 May outage, the Police Assistance Line 131 444 telephone number that is used by Police services in each State and Territory (except Victoria) was widely publicised (by NSW Police) as an alternative telephone number to call. The publication of this number presented confusion to Victorian residents that were unable to access the service (Victoria will commence using this number in 2019).

Resilience of the ECS would be improved with the availability of alternative backup numbers that can be called by the public in the event of a disruption to the Triple Zero number/service. These numbers should utilise an alternative carrier network to the network utilised by the ECP, and be available for immediate use should the need arise (the numbers should be active, and connections to each ESO established ready for use). A different '13' or '1800' contact number should be available for Police to use nationwide, Ambulance services to use nationwide, and Fire services to use nationwide (three separate numbers that are preconditioned to route calls to the correct State/Territory Police, Fire or Ambulance service based on the location of the caller).

Recommendation 7

The ECP for Triple Zero to work with the Triple Zero Coordination Committee to investigate providing alternative contact numbers to facilitate calls to ESOs that can be utilised in the event of a disruption to Triple Zero services. These numbers should only be publicised in the event of a disruption to the Triple Zero service.

The outage of 3 and 4 May 2018, and the incident of 26 May 2018, demonstrated that there is room for improvement in the way that Telstra handles disruptions to the Triple Zero ECS. In addition, work is needed within each State/Territory to ensure that communication is optimised within those jurisdictions between ESOs, public safety agencies and government departments with a relevant interest in the provision of emergency services. While it is recognised that plans already exist at the State/Territory level, the events investigated in this report present an opportunity to revise existing arrangements. The draft NECWG-A/NZ protocols note that ESOs should identify a single point of contact within their agency for the duration of the disruption, and review current redundancy processes, systems and plans to manage a national or State/Territory disruption.

Recommendation 8

State and Territory ESOs and their respective government agencies should review their current business continuity and disaster recovery arrangements to ensure there are adequate processes in place to manage incidents within each jurisdiction, including the management of media messaging and communications to the public during a disruption to the Triple Zero service (that is coordinated with the processes set out in the Triple Zero Disruption Protocols).

Without pre-empting the findings of the ACMA's investigation of Telstra's compliance with regulatory requirements imposed by the ECS Determination or the Emergency Call Service Requirements Industry Code (C536:2011), DoCA considers that it is timely, given the significant importance of the Triple Zero service, to review the regulatory protections available to the Australian community to ensure they are adequate. Improved protections would need to be reflected in the ECS Determination, the Industry Code, and contractual arrangements managed by DoCA.

Recommendation 9

That the ACMA review the Telecommunications (Emergency Call Service) Determination 2009 to ensure that the Determination:

- ***provides adequate protections to the Australian community;***
- ***takes into account market and technology changes;***
- ***imposes clear and consistent obligations across the ECS supply chain;***
- ***includes a requirement for timely and effective communication across the ECS supply chain when there is a disruption to emergency services.***

As part of the review, the ACMA considers whether any parts of the C536:2011 Emergency Call Service Requirements Industry Code and the G644:2011 Emergency Call Service Requirements Guideline should now be included in the Determination.

Recommendation 10

That the Communications Alliance review the C536:2011 Emergency Call Service Requirements Industry Code and the G644:2011 Emergency Call Service Requirements Guideline (which provides guidance in the event of a DoS attack to the Triple Zero service) to ensure the code and guideline:

- ***provide adequate protections to the Australian community;***
- ***take into account market and technology changes;***
- ***impose clear and consistent obligations or guidance across the ECS supply chain.***

In light of the other findings and recommendations of this report, the TZCC, chaired by the Department of Communications and the Arts, should also review the terms of reference of the committee to ensure that gaps in service delivery, or risks to successful end-to-end service delivery are identified and addressed. The committee should review the gap analysis and risk analysis at least twice a year at committee meetings.

Recommendation 11

The Department of Communications and the Arts should review the terms of reference for the Triple Zero Coordination Committee to ensure the committee has a proactive role in identifying and resolving gaps and risks to end-to-end service delivery for the Triple Zero Emergency Call Service and establish a clear work program to address these.