Triple Zero Legislative and Regulatory Review Consultation

Triple Zero Custodian

June 30, 2026

Public

TPG Telecom Limited ABN 76 096 304 620

Level 27, Tower Two, International Towers Sydney, 200 Barangaroo Avenue, Barangaroo NSW, 2000

Submission

TPG Telecom (**TPG**) welcomes the opportunity to provide a submission in response to the Triple Zero Legislative and Regulatory Review Consultation.

Additionally, TPG supports and participated in the development of the Australian Telecommunications Alliance (**ATA**) submission.

About TPG Telecom

TPG Telecom Limited is a leading challenger full-service telecommunications provider and owns and operates a nationwide mobile network that is connecting Australia for the better. We operate leading mobile and internet brands including Vodafone, TPG, iiNet, Lebara and felix mobile.

Executive Summary

The current emergency communications framework spans multiple legislative and regulatory instruments, resulting in a complex and, at times, fragmented environment with overlapping obligations and accountabilities. This review presents an important opportunity to streamline and clarify the regulatory landscape, strengthen coordination across stakeholders, and ensure that governance arrangements are coherent, consistent, and effective in supporting the end-to-end delivery of emergency communications across Australia.

TPG supports a modernised framework that is clear, proportionate and aligned to operational control. Carriers and CSPs have made and continue to make significant investments in network monitoring, testing, contingency planning and incident response, and have established systems and processes to support the delivery of emergency call services. However, emergency communications operate across a multi-party ecosystem, including devices, the Emergency Call Person (**ECP**) and Emergency Service Organisations (**ESOs**). The framework must reflect this reality by ensuring obligations are assigned to the parties best placed to manage risk, and that liability is not extended beyond a party's reasonable sphere of control.

The framework must also support future evolution while maintaining reliability and redundancy as core principles of the Triple Zero service. Voice should remain the primary channel, with additional contact methods introduced only where they meet defined reliability thresholds and are supported by appropriate investment and enforceable rules, including support for ESO capability and clearer device manufacturer obligations. A flexible, technology-agnostic legislative framework, supported by a mix of industry standards and codes, will provide the necessary adaptability while maintaining clear and enforceable outcomes.

Finally, effective coordination and information sharing across the ecosystem will be critical to delivering a reliable and future-proof emergency communications system. This includes further developing the role of the Triple Zero Custodian, improving consistency across reporting and notification requirements, and supporting coordination and support during disruptions to emergency communications.

Together, these reforms will support a more resilient, coordinated, and user-focused emergency communications framework.

Responses to specific questions

Question 1: What principles should guide Triple Zero service regulation in the contemporary telecommunications environment? How should these be reflected in the legislative and regulatory framework?

- Clear and consistent terminology: All emergency communication-related legislative and regulatory instruments should adopt aligned, unambiguous definitions and consistent terminology. Inconsistent definitions result in inconsistent and complicated application in practice. This has been illustrated in the misalignment between the *Telecommunications (Emergency Call Service) Determination 2019* (**ECSD**) and *Telecommunications (Customer Communications for Outages) Industry Standard 2024* (**CCO Standard**) in relation to outage notifications.
- End to end enforcement powers: To maintain the integrity of emergency communications access, all parties involved in delivery of that ecosystem should be included in the future framework. This includes the need for the ACMA to be empowered to manage a compliant device register, based on information shared collaboratively between Carriers, Carriage Service Providers (**CSPs**), and device manufacturers.
- Proportionality and control: Obligations on Carriers and CSPs must be proportionate to the level of control they have over the relevant risk, and data available to support compliance. Given emergency communications depend on multiple parties, responsibilities and obligations should be clearly allocated and applied to the relevant party best placed to manage that risk.
- Timeliness: We recognise the importance of delivering timely changes into the emergency communications ecosystem, however any compliance or change timeline must be reasonable and consider the risks of rushed delivery. Failure to consider if a timeline is technically possible risks placing pressure into the ecosystem.
- Technology agnostic and flexible framework: Emergency communication regulation should remain, to the extent possible, technology agnostic to support network evolution and modernisation. The framework should allow for Carriers and CSPs to continue to upgrade and modernise their networks and support service delivery as network changes are delivered. These changes will also enable and support potential modernisation of emergency communications options.
- Incorporation of industry guidance and technical specifications: The review should also take into account relevant ATA guidelines to ensure consistency with existing industry practice. This is particularly important where clear and consistent terminology is required, such as the increased use of technically defined terms (e.g., the use of call failure codes, rather than descriptions of ‘graceful’ and ‘ungraceful’ calls). It should also consider materials and guidelines developed for connection into emergency services, including those developed and published by the National Emergency Services Working Group (**NECWG**).
- Embedding engagement and information sharing: There must be an established function to support cross-collaboration across the emergency communications ecosystem. NECWG is a well established and trusted example of operational collaboration, however an equivalent mechanism to support a decision-making body is needed. The Triple Zero Coordination Committee has provided some level of support; however, it has not functioned as intended. Learnings should be considered from the successes of the National Road Safety Strategy and the Office of Road Safety Branch to manage consistency and co-ordination across Federal, State and Territory level of government.
- International learnings: Consideration should be given to established approaches in North America and Europe, including alignment with EENA and NENA principles and standards where relevant. This is particularly relevant for modernisation of Australian systems and interoperability

of new and emerging technologies for emergency communications and emergency response. Additionally, public-facing concepts should be considered for the Australian environment, including a public 'test' number. Having a publicly available test number would allow the public to 'check' on the availability of an emergency voice service. In the United States, this is achieved by the use of a designated number - 993. When 933 is dialled, the call follows a similar network path to a real 911 call, however before connecting to a Public Safety Answering Point (PSAP), the call is intercepted and routed to an automated system (an IVR). This allows the public to confirm whether the call would route correctly and that their service is properly provisioned, without creating failed or short calls that may trigger actions such as welfare checks by Carriers or the ECP.

Question 2: Are there any barriers in the current legislative and regulatory framework blocking access to the benefits of new delivery technologies which could be used to contact Triple Zero? If so, what aspects of the legislative and regulatory framework need to be amended to increase flexibility?

TPG supports the introduction of multi-modal access to emergency communications. However, we recognise the practical challenges associated with delivery, including the risk of inconsistent implementation in the absence of a national strategy, as well as cost and network capacity constraints.

The current legislative and regulatory framework for emergency communications is not fit for purpose in a multi-modal environment. It is primarily designed around voice services (delivered via fixed and mobile networks), with limited accommodation for non-voice channels through the Text Emergency Relay Service (106). Integrating new communication methods (such as SMS, MMS, RCS, data services and data enabled over-the-top (**OTT**) applications) would require more than incremental amendments to existing rules. A fundamental shift in regulatory approach is required.

Non-voice services should not be viewed as a replacement for voice, but as complementary channels that enhance accessibility, provide redundancy, and support user choice. Research conducted by Motorola Solutions on behalf of NECWG indicates continued reliance on voice across all demographic groups, while also demonstrating a growing expectation that additional contact methods, particularly SMS and app-based services, will be available.[1]

Given the differing technical characteristics and user applications of non-voice services, a future framework should focus on end-to-end service outcomes rather than prescribing specific technologies or forcing action by telecommunication providers. In particular, the framework should prioritise the effective, reliable and consistent delivery of emergency communications across all supported channels across the ecosystem, from Carriers, CSPs, and ECP to support connecting to the ESOs to support dispatch and response.

To enable this, we recommend adopting a flexible, layered regulatory model that utilises the full range of available legal instruments. This would include:

- Primary legislation to establish that emergency communications may be delivered via multiple technologies beyond voice,
- Industry codes and standards to define technical requirements, operational processes and service expectations, and

[1] *Attachment A Motorola Solutions NECWG 2026 Presentation; NECWG May 2026 Presentations*

- Guidance and regulatory oversight via Standard to support consistency, interoperability and consumer outcomes.

A mixed-instrument approach would ensure that obligations are set at the appropriate level, enabling technical rules to evolve over time while maintaining clear, enforceable outcomes. This structure would enable those best suited - be it industry, government, or the regulator - to develop requirements that are practical and fit for purpose, capable of supporting stable and accessible emergency communications for all Australians.

Question 3: How should the legislative and regulatory framework balance multi-modal access to Triple Zero, when compared to reliability and redundancy?

Prioritisation of reliability must remain the central focus of any modernised emergency communications framework. Legislative and regulatory settings should balance the benefits of multi-modal access with the need to maintain reliability and redundancy, ensuring the integrity of the Triple Zero service is not compromised. New access channels should be treated as supplementary to voice, rather than a replacement, and only introduced where they meet defined reliability and resilience thresholds informed by technical standards and operational experience.

This balance requires a clear delineation of roles and responsibilities across the emergency communications ecosystem, and a framework that aligns obligations with operational control. Carriers are responsible for building and maintaining network infrastructure that processes, routes, and transmits communications, but do not directly engage with the public. CSPs enable their customers to connect to the Carrier's network, however, cannot easily control the devices used to connect. Where multi-modal access is enabled, Carrier and CSP obligations in relation to failed contact attempts must be clear. For example, Carriers and CSPs do not have control of data-enabled OTT communications and cannot reasonably manage risk or performance outcomes for such services.

Multi-modal access should enhance the reliability of the system by providing additional pathways to access ESO's. Where new channels introduce uncertainty (for example, OTT integration may cause issues in response times, location information, or delivery assurance), the framework should prioritise the integrity of emergency communication and effective delivery of new capability over a focus on multiple forms of access.

Any expansion must also be supported by complementary investment in ESO capability and appropriate inclusion of device manufacturers within the regulatory framework. Voice should remain the primary and most resilient channel, with alternative pathways designed to support accessibility without creating additional points of failure or diverting resources from core service delivery.

Question 4: Should the legislative and regulatory framework allow for the ACMA, and/or the Minister, to determine which class of devices or technologies should or should not be able to reach Triple Zero, in order to safeguard the integrity of access for the system?

We are supportive of the ACMA being empowered to identify classes of device or technologies which should or should not be able to connect into the emergency communication ecosystem. However, any determination by the ACMA should be made in conjunction with Carriers and CSPs, as well as device manufacturers, to ensure it is capable of being complied with by the impacted parties and is based on technical and device level specifications. This approach supports the integrity of access by ensuring

only devices capable of reliably connecting to emergency services are permitted, while avoiding inconsistent or fragmented implementation.

Carriers and CSPs are responsible only for the networks they provide. They do not manufacturer or control the devices on the network or whether such devices are capable of being able to reach Triple Zero. As the issues with Part 4 of the ECSD has shown, there are significant numbers of devices that are brought into and used by end users in Australia, including devices designed for non-Australian markets. End users of these devices may be in Australia for a short or medium period of time on holiday or working visa, may be a citizen or permanent resident who purchased the device while travelling overseas, or may have purchased the device in Australia via a non-telco retailer who is unaware the device is not capable of connecting to emergency services.

The current provisions of Part 4 of the ECSD place significant burden on Carriers and CSPs to understand the operation of an inordinate number of and type of device. TPG is supportive of solutions that provide a consistent approach across Carriers to determining the capability (or not) of devices to access Triple Zero, as well as requiring the support of manufacturers. For example, the establishment of a mobile device register by ACMA which identifies compliant devices. This would support greater consistency across the Carriers, with an ACMA register providing a mechanism for technical alignment.

Question 5: Should mobile device manufacturers be considered more centrally in the Triple Zero legislative and regulatory framework (such as under the ECS Determination)? What, if any, additional requirements should apply to mobile device manufacturers to ensure mobile devices can reliably contact Triple Zero on Australian networks?

TPG supports mobile device manufacturers being incorporated into the emergency communications legislative and regulatory framework. This is necessary to support reliability and consistency for consumers, and to reflect the increasing role of devices in enabling network access, particularly as multi-modal communication methods are introduced. This includes the need to look beyond mobile devices.

As other access methods are incorporated, consideration must be given to the inclusion of wearables, smart house devices, smart cars, and other device type that will increasingly seek to connect to emergency services on behalf of their end users. This is happening today in a haphazard way. An example of a non-mobile device connectivity type that has sought to engage with the ESOs is the use of NECWG guideline "*A National Protocol for Vehicle Alert Escalation contact with Triple Zero (000)"* by the Australasian New Car Assessment Program (ANCAP) in the refreshed ANCAP Assessment 2026-2028, to support emergency call and automatic crash notifications.[2]

These could include requirements for manufacturers to respond to information requests from Carriers and CSPs in relation to emergency call compatibility, undertake testing of devices on Australian networks (including for emerging communication methods), and promptly notify relevant parties of any known issues affecting emergency connectivity. Manufacturers should also meet defined technical requirements for access and to address identified device issues, including for newer technologies and

[2] Australasian New Car Assessment Program (ANCAP) ANCAP Assessment 2026-2028, https://www.ancap.com.au/how-is-vehicle-safety-changing

system configurations, and provide relevant information to a centrally managed register of device capability (hosted by the ACMA).

In addition, manufacturers should be required to provide clear information to consumers regarding device capability and any limitations that may impact access to emergency services. This may include, for example, scenarios where device settings (such as VoLTE or Wi-Fi calling) affect the ability to make emergency calls. Consideration should also be given to requiring devices to be configured, by default, in a manner that supports reliable emergency connectivity, with users retaining the ability to modify these settings if they choose. Strengthening manufacturer obligations in this way would support a more consistent and reliable end-to-end emergency communications ecosystem, while ensuring accountability sits with the parties best placed to manage device performance.

However, any expansion to directly include device manufacturers should be accompanied by appropriate safe harbour provisions for Carriers and CSPs where emergency communication is impacted by circumstances outside their reasonable control. This include device design, software configuration, manufacture updates, or the operation of third party elements. The safe harbour provision for telecommunication providers would promote clear accountability sits with the parties that can best manage that risk.

We acknowledge that some of this activity will require international engagement and alignment, as relevant standards and technical specifications are established globally.

Question 6: What outcomes should carriers, CSPs and ECPs be accountable for in delivering Triple Zero calls, and what minimum requirements are needed to achieve those outcomes?

Carriers and CSPs should be accountable for ensuring that emergency communications made via their networks are transmitted, routed, and delivered to the termination point for connection to the ECP reliably and without avoidable interruption. These obligations should be framed in a way that reflects the technical complexity of modern networks and the broader emergency communications ecosystem and must be limited to matters within the reasonable control of Carriers and CSPs.

We strongly support the position in the ATA submission that the framework should avoid creating an expectation that Carriers or CSPs can guarantee connectivity in all circumstances, particularly where issues arise from unsupported devices, unknown software configurations, or non-compliant equipment. Given the technically complex nature of the ecosystem, accountability and minimum requirements must be aligned to areas within the control of the regulated party.

The framework should avoid imposing strict liability where performance outcomes are affected by factors outside a provider's knowledge or control, including device limitations, third-party applications, safe harbours for planned maintenance, or unforeseen network interactions. This includes during the introduction of any new access or service types into the emergency communications ecosystem.

To support this, the operation of the "beyond the control" exception in section 19 of the ECSD should be clarified and broadened. In particular, the framework should recognise that where the root or dominant cause of an outage is unknown, could not reasonably have been anticipated, or is not detectable through standard network management, the exception should apply. The current formulation sets a higher standard than the "maintain as far as practicable" obligation in section 11, and these provisions should not be interpreted in a way that narrows the intended operation of section 19. Greater consistency is also needed across the ECSD, including alignment between section 19 and

Part 4, to ensure obligations are applied coherently across different technologies and network types.

Minimum requirements for Carriers and CSPs should focus on ensuring effective end-to-end delivery within the direct control of the relevant Carrier or CSP, supported by clear and consistent rules. This includes defining responsibilities for call routing, fault detection and remediation. Consideration should also be given to the broader policy approach for edge cases, including whether it is preferable to restrict device access where emergency calling capability cannot be assured, or to allow continued service with clear consumer warnings regarding limitations.

Question 7: How could the framework be amended to further provide obligations to support the proactive identification and rectification of systemic issues? What mechanisms (for example, incident learnings, mandatory improvement plans, directions, audits) are most effective, and why?

TPG (and other Carriers) undertake extensive network monitoring, testing, and contingency planning to identify and address issues proactively. Any amendments to the framework should build on these existing practices rather than duplicate them. Additional obligations should be proportionate, targeted, and aligned to areas within the reasonable control of Carriers and CSPs and should not introduce inconsistency with existing requirements or create regulatory uncertainty. Once again, we recommend close alignment with industry in the establishment of any new rules or standards, to ensure that what is developed is based on clear, targeted technical specifications.

The framework should focus on mechanisms that support continuous improvement and the effective identification of systemic issues. This includes structured incident review processes, clear expectations around the capture and sharing of learnings, and targeted remediation steps where systemic issues are identified. Mechanisms such as improvement plans or regulatory directions may be appropriate where there is evidence of recurring or material issues but should be applied in a risk-based way that avoids unnecessary regulatory burden or detrimental operational impacts. They should be considered an option of last resort.

In implementing these mechanisms, the framework should remain sufficiently flexible to accommodate evolving technologies and operating models, including the use of automation and artificial intelligence to support network monitoring and incident response at scale. Care should be taken to ensure that regulatory settings do not unintentionally limit the use of these tools, particularly where they improve the timeliness and effectiveness of issue identification and resolution. Clear definitions and guidance, including in relation to AI-enabled processes, would assist in providing certainty and supporting consistent application across industry.

Question 8: Should new and ongoing performance reporting for carriers and/or CSPs providing access to Triple Zero be introduced? If yes, what metrics should be reported and how often?

TPG supports the introduction of performance reporting where it is proportionate, targeted, and delivers meaningful insights into the system's performance. The current reporting provided to the Triple Zero Custodian under direction has provided initial insights for emergency calling and welfare check performance by the relevant Carriers. Any additional reporting obligations should take into account the data reasonably available to Carriers and CSPs. It should also consider the data available as part of the independent testing being done in collaboration with Carriers at the University of Technology Sydney's National Telecommunications Resilience Centre. Any new performance

reporting should focus on outcomes, rather than a prescriptive focus on internal processes or remediation steps which may not reflect overall system performance.

A key priority should be improving consistency and clarity across the existing reporting framework. There is currently a fragmented set of obligations across multiple instruments, including the ECSD and CCO Standard, which use inconsistent terminology and categorisation. This creates complexity and increases the risk of duplicative or overlapping reporting requirements. The use of 'descriptive' requests will result in different outputs from different Carriers and CSPs, where the use of technical code would result in a more repeatable and consistent data set. Greater alignment is needed, including clear definitions of outage categories, call failure types, welfare check types, to support standardised reporting thresholds across industry. The new reporting provided under direction provides an opportunity to create consistency of output across the parties, before moving to any new legal or regulatory performance reporting rules.

Reporting obligations should also be designed to avoid duplication in notification and escalation requirements, and to minimise administrative burden while still supporting regulatory oversight. Consideration should be given to a streamlined framework that consolidates reporting obligations and enables regulators to monitor trends and systemic issues effectively, without imposing unnecessary or repetitive reporting requirements on Carriers and CSPs.

Question 9: What information is and should be shared across industry and/or ESOs to support the proactive, reliable and future-proof delivery of Triple Zero. What governance arrangements are needed to enable timely, secure and usable information sharing?

The framework should give consideration firstly to why any information or data is being shared. Is the intent to share information or data with the ACMA in its role of providing regulatory oversight of the Carriers and CSPs, or is it with the role of Triple Zero Custodian to support and provide overarching coordination and oversight of the emergency communications ecosystem? Data sharing should not be just about information – it must be informed by purpose.

For example, a centrally controlled and monitored device register identifying devices considered configured to be able to access emergency service maintained by the ACMA, may include a need to collaborate with device manufacturers, Carriers, and CSPs to support the ACMA in its management of the register when it becomes aware of a connectivity issue. This supports all parties involved to act and manage the risks associated with a non-compliant device in a centralised and clear way.

Governance arrangements would need to be customised to the reason for the sharing of data. For the Triple Zero Custodian, we strongly encourage consideration of the position by the Department of Home Affairs National Office of Cyber Security (**NOCS**) in its engagements with industry. The clear delineation between the NOCS and regulatory enforcement means it engages with relevant stakeholders in a way that is focused on enabling timely, secure, and usable information both in the moment of crisis and in the normal course of business. By cultivating this approach, the NOCS has developed an approach that supports proactive disclosure and effective engagement with industry. A level of safe harbour for disclosure is vital to the Triple Zero Custodian to support its function of overarching coordination and oversight. Not all issues that emerge will be connected to a regulatory breach or issue, so reliance on enforceable information gathering powers and audit questions will not result in the Custodian having a clear picture of all parts of the emergency communications ecosystem.

Question 10: Does the objective of the single national emergency call system encourage, or hinder, the ability for state and territory organisations to innovate in their delivery of emergency calling and dispatch services?

Question 11: Is there information that carriers, CSPs, and ECPs hold which is not currently, but should be made available to ESOs through regulation to support the delivery of emergency services?

TPG supports the development of a framework that enables the ESOs to innovate and develop dispatch services that are suited to their conditions and functions. However, such innovations do rely on connectivity services that are not designated emergency service and therefore sit within our normal service operation areas. Any multi-modal approach developed by this framework should support consistency across Australia, backed by technical supports that deliver the resiliency and redundancy Australian's expect from emergency services.

Again, the end-to-end visibility and support is something that the Triple Zero Custodian should seek to enhance. The Triple Zero Coordination Committee has provided some level of support, however, it has not functioned as intended. Learnings should be considered from the successes of the National Road Safety Strategy and the Office of Road Safety Branch to manage consistency and co-ordination across Federal, State and Territory level of government.

Question 12: Are there any additional regulatory powers and mechanisms the ACMA requires to regulate Triple Zero, especially to support a framework which is proactive and future-focused?

As noted above, we are of the view the ACMA should control and manage a register of compliant devices for the purpose of Part 4 of the ECSD.

We are also supportive of changes to the legislative and regulatory framework to clearly incorporate device manufacturers within the ACMA's remit for the purpose of emergency communications.

Question 13: Are there barriers to the ACMA considering systemic Triple Zero issues, or linking related infringements, to ensure issues indicating broader problems are addressed appropriately? If yes, what should change?

We note that there remains concern in public statements from consumer groups about the powers of the ACMA. In addition to the inclusion of device manufacturers as outlined above, we support the passage of the *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* ***(ECS Bill*****).** This would provide the ACMA with greater enforcement powers, while supporting the role of industry codes. As outlined above, effective regulation is best achieved where legislation, direct regulation (via Standards), and co-regulation (via Codes and guidelines) are used in a coordinated and strategic manner.

Even with the passage of the ECS Bill, the powers of the ACMA will remain focused on the 'up stream' elements of the emergency communication ecosystem – Carriers, CSPs, the ECP and potentially device manufacturers. They will have no jurisdiction over the full end-to-end system, being ESOs. This is a function of federation, which requires the Triple Zero Custodian to engage with in its new functions.

Question 14: Do recent changes to the TCPSS Act effectively balance the role of the ACMA as a regulator with the role of the Custodian as an entity which oversees the Triple Zero ecosystem as a whole?

Yes, however as noted above, there must be clear distinction in the actions taken by the Triple Zero Custodian between knowledge gathering and any quasi-investigation activity. We acknowledge that the Custodian staff are in a development stage, however duplication between the activity of the ACMA and the Custodian must be avoided, to reduce regulatory burden and support the effective and efficient provisioning of accurate information.

For example, the Custodian has asked Carriers to inform them of incidents under the *Custodian Triple Zero Notification Protocol*, which was provided unilaterally to Carriers by Custodian staff. This is in addition to our regulatory requirement to inform the Custodian under the ACMA's enforceable *Telecommunications (Customer Communications for Outages) Industry Standard 2024*. This is the kind of inconsistency that creates confusion during major events, teams focus on meeting mandatory timelines and contact pathways. It is not clear what the Custodian staff will do with the information if provided under the Protocol and what support for coordination and collaboration would be available.

Question 15: Does the Triple Zero Custodian have all the powers needed to fulfil its functions under the TCPSS Act?

At this time, with the Triple Zero Custodian so newly established, there is no indication that the Custodian has not been granted sufficient powers.

Rather than seeking more powers, we strongly recommend that the Custodian staff engage with impacted parties on how they will be bringing to life the powers under section 151K(1)(a) (aiding preparation for, response to or recovery from an ECS outage event). This coordination function is essential, particularly for the end-to-end engagement and to support the flow of information during an outage. No protocol currently exists on how the Custodian would provide support to respond to or recover from an ECS outage event. Relevant activity may include supporting the ECP and ESOs to connect to the relevant Carrier and impacted CSPs, supporting public awareness and public-facing information for alternatives for assistance, assistance in welfare check coordination, or engagement with other government departments.

Other areas of concern

Welfare checks

TPG supports the need for welfare checks and treats this obligation seriously. A welfare check reflects a failed attempt to contact emergency services, and we have established processes, systems and staff training to respond where required that exceeds the requirements in regulation.

However, the current approach would benefit from review. CSP's and Carriers are limited in the service they can provide as part of a welfare check.

Carriers and CSPs are responsible for the transmission and routing of communications but do not have a direct connection into the relevant ESO. While TPG currently undertakes welfare checks during major outages, these are necessarily limited to confirming whether assistance is still required and directing the caller to reattempt contact with emergency services where appropriate. We do not support CSP staff undertaking broader assessments of a caller's health or safety, as this extends beyond their capability and risks delaying connection with trained ECP or ESO personnel.

Feedback from ESOs highlights a number of challenges with the current approach, including limited caller information, lack of reliable location data, duplication where callers have already connected, and cases where escalation does not result in an emergency response. .

We consider that welfare check obligations should sit with the ECP, as the entity best placed to assess failed or incomplete contact attempts and determine whether further action is required. This would require appropriate resourcing of the ECP and clear rules to support the provision of relevant information from Carriers and CSPs.

A model where the ECP manages welfare checks would support a more consistent, coordinated, and effective approach across the emergency communications ecosystem.

Network redundancy

The *Investigation Report into the Triple Zero Service Disruptions of 4 & 26 May 2018* [3]recommended that there should be additional network redundancy in the Triple Zero ecosystem.

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).*

TPG has sought to provide direct access to the Emergency Call Person to provide such redundancy but has so far met resistance.

The network redundancy between the ECP and ESO's also needs revisiting.

---

3 https://www.infrastructure.gov.au/sites/default/files/investigation_report_into_the_triple_zero_service_disruptions_of_4_26_may_2018_1.pdf