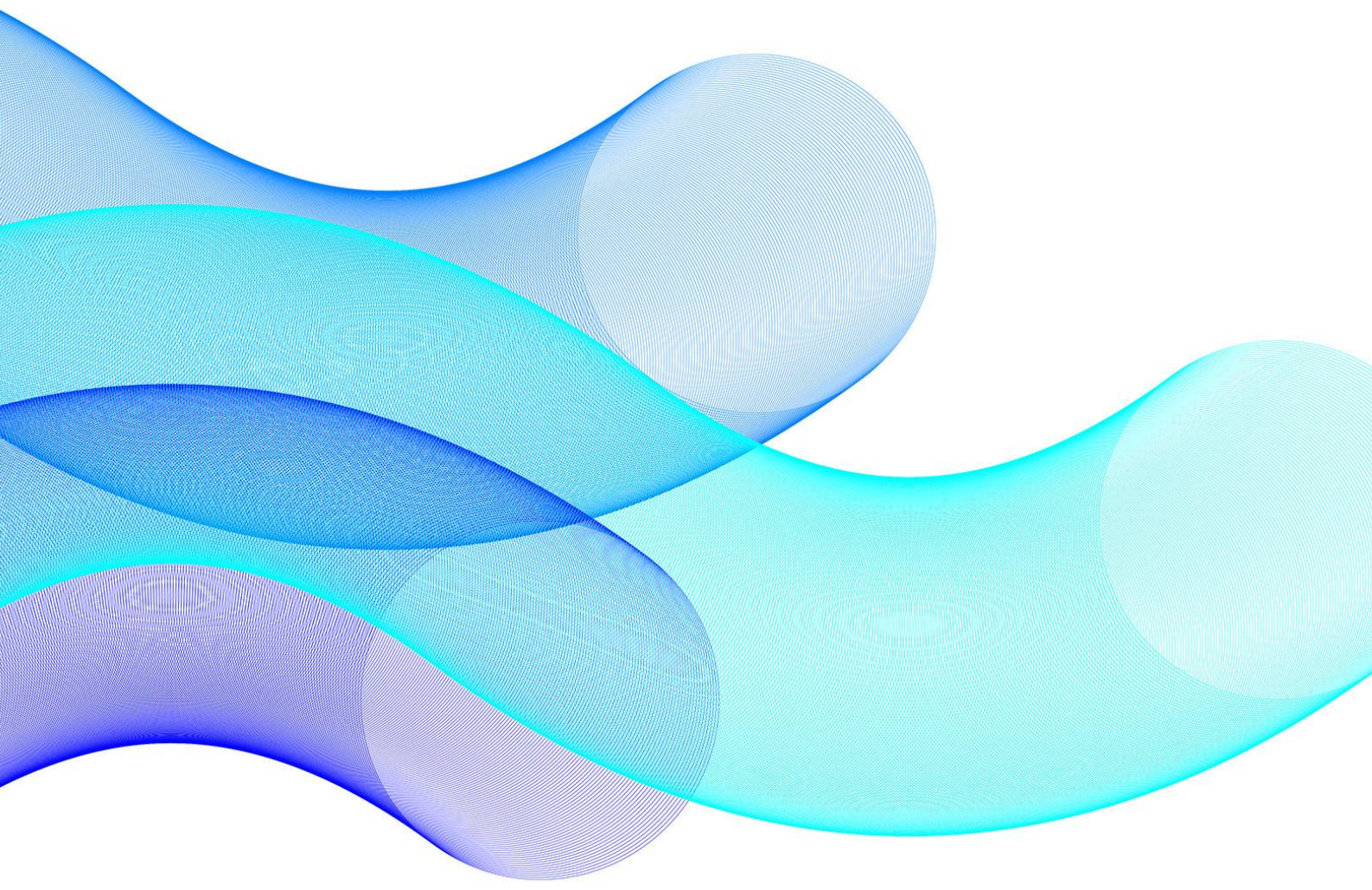
Vocus Submission

Triple Zero Legislative & Regulatory Review

30 June 2026



Vocus Group Limited | ABN 96 084 115 499 | vocus.com.au
Level 10, 452 Flinders Street, Melbourne, VIC 3000

About Vocus

Vocus, Australia's specialist fibre and network solutions provider, owns and operates 50,000km of secure, high-capacity fibre connecting all Australian mainland capitals with New Zealand, Asia, and the USA. Beyond the fibre network, Vocus operates a growing network of submarine cables spanning nearly 15,000kms that includes the Australia Singapore Cable, North-West Cable system, the Darwin-Jakarta-Singapore system, and the PPC-1 cable from Sydney to Guam.

Vocus' national fibre backbone also provides the foundational infrastructure for Starlink's Low Earth Orbit (LEO) satellite service – enabling revolutionary high-speed connectivity to 100% of Australia's landmass, no matter how remote.

Vocus owns a portfolio of well recognised brands catering to enterprise, government, wholesale, small business and residential customers across Australia. For more information, visit vocus.com.au.

Executive summary

Vocus welcomes the opportunity to respond to the Triple Zero Custodian (Custodian)'s '*Triple Zero Legislative and Regulatory Review*'.

Vocus is committed to working collaboratively with the Custodian, Australian Communications and Media Authority (ACMA) and industry to strengthen the reliability and delivery of Triple Zero. This submission sets out priority recommendations to uplift the legislative and regulatory framework:

(1) **Centralise coordination under the Custodian.** Vocus strongly recommends delineating the Custodian's role from that of the ACMA as regulator. The Custodian should operate as a trusted hub for information exchange and operational coordination during unplanned outages. To enable this, we recommend introducing limited-use information sharing obligations, modelled on those established for the National Cyber Security Coordinator (NCSC) under the *Cyber Security Act 2024* (Cth).

(2) **Prioritise targeted reform of the existing framework**, as opposed to introducing new overlapping and/or duplicative obligations. This should include:

   a. **Streamlining regulatory notifications**: Reconcile the requirements in the *Telecommunications (Customer Communications for Outages) Industry Standard 2024* (TCCO) and *Telecommunications Emergency Call Service Determination 2019* (Cth) (ECS) with the Custodian's Triple Zero Notification Protocol. There should be a single, consistent notification pathway for unplanned outages to enable efficient reporting while allowing operational teams to focus on restoring services.

   b. **Clarify roles and expectations for welfare checks**: The entity that has the direct relationship with the end-user and has access to their name, number and address should perform the welfare check. This should be supported by establishing a Carriage Service Provider (CSP) register.

   c. **Leverage existing frameworks to improve Triple Zero risk management**: Undertake a holistic review of existing Triple Zero risk management obligations before introducing new requirements. Clarify how obligations under the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP) apply to Triple Zero risk management.

   d. **Clarify expectations about Management Plans under section 80 of the ECS:** Deliver practical guidance on the types of changes that are intended to trigger section 80 of the ECS.

Vocus welcomes the opportunity to continue to uplift the legislative and regulatory framework to deliver more reliable, trusted Triple Zero services to Australian communities.

Priority recommendations to deliver trust in Triple Zero

(1) Centralise coordination under the Custodian

Since its establishment in August 2025, the Custodian has played an important role in engaging industry stakeholders to improve the management of the Triple Zero ecosystem. Building on this foundation, there is now a clear opportunity to mature the role of the Custodian to act as a trusted hub for information exchange and operational coordination during unplanned outages.

Centralising coordination also provides an opportunity to clarify other roles within the framework. There is currently ambiguity between the respective roles of the Custodian and the ACMA. This can be addressed by maintaining the ACMA's role as the regulator and enforcement body, while positioning the Custodian as a collaborative, coordination-focused entity working with industry to improve outcomes.

The role of the NCSC provides a useful model. The NCSC leads whole-of-government responses to significant cyber incidents, supported by provisions in the *Cyber Security Act 2024* (Cth) that enable organisations to share information on a limited-use basis.[1] This means information can be provided to support coordination and response without it being automatically used for regulatory or enforcement action. While this does not remove legal obligations or liability, it creates a more trusted environment for timely, transparent and confident information sharing during incidents.

Importantly, this reform should focus on enabling better information sharing – not simply more information sharing. Industry urgently needs clarity on what should be shared, with whom, for what purpose and under what controls. Given the number of stakeholders involved in end-to-end emergency service delivery, a clearly defined coordination point – separate from enforcement – would materially improve the information flow during network outages and critical events.

Recommendation: Vocus recommends that the Custodian be formally responsible for collecting, validating and sharing operational data across all participants, including carriers, CSPs, the Emergency Call Person (ECP), Emergency Service Organisations (ESOs), the ACMA and government. This should be underpinned by clearly defined, standardised information flows, with agreed triggers, data fields and formats.

As a practical step, the Custodian (TripleZeroCustodian@infrastructure.gov.au) should be added as a 'relevant stakeholder' under TCCO and ECS, ensuring it has visibility over all Major Outage and Significant Local Outage notifications. In this role, the Custodian should operate as a single source of truth for system status, outages, risks, incidents, planned changes and key communications, supported by a managed, end-to-end system dashboard.

(2) Prioritise targeted reform of the existing framework

Over the past two years, the telecommunications sector has undergone significant reform to outage management regulation, including amendments to the TCCO, ECS, and the introduction of the TSRMP Rules. While these changes represent a substantial uplift in obligations, there has been no holistic post-implementation assessment of how these frameworks interact or whether they are collectively improving network resilience and access to Triple Zero.

Given the scale of reform and the significant investment by industry in systems, processes, and operational capability to meet these requirements, it is essential to improve the existing framework before introducing new obligations. We have outlined priority recommendations below.

[1] Australian Government National Office of Cyber Security, '*Factsheet: Limited use for the National Cyber Security Coordinator*' <https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-limited-use-for-the-national-cyber-security-coordinator.pdf>.

A. Streamline notification protocols

Vocus has previously outlined concerns with the TCCO and ECS notification framework, particularly the practical difficulty of identifying Major Outages and Significant Local Outages where services do not have a clearly defined geographic location.[2]

In 2024, the Office of Impact Analysis estimated that implementing the TCCO Major Outage requirements would cost industry approximately $117 million over ten years.[3] Given these substantial investments, any further changes should be carefully designed to build on and integrate with existing processes, rather than introduce duplicative or overlapping requirements.

Vocus remains committed to ensuring the Custodian has access to the information it requires to perform its role effectively. However, the recently issued Triple Zero Notification Protocol raises several concerns, including the subjectivity of certain notification triggers and the challenges this creates for consistent interpretation by operational teams. Without clearer parameters, there is a real risk of inconsistent reporting and confusion during live incidents, which is likely to ultimately detract focus from incident response efforts.

For example, further guidance is required on the scope of triggers such as 'when a systemic network, systems or other issue has been identified that is impacting, or may impact, the carriage of Triple Zero calls, but is not covered by existing regulatory frameworks.'[4] Similarly, the trigger capturing 'any other issue that may bring the integrity or trust in the Triple Zero system into question' is inherently broad and subjective.[5] Without non-exhaustive examples, thresholds, or other objective criteria, these triggers cannot be operationalised effectively, particularly in time-critical outage scenarios where frontline teams must make rapid decisions.

Vocus therefore seeks clarification on how the Triple Zero Notification Protocol is intended to interact with the existing TCCO and ECS notification obligations. It is also unclear whether the new Triple Zero Failure Notification Form is intended to operate in parallel with, or in addition to, existing notification requirements for Major Outage and Significant Local Outage. This creates a significant risk of duplication and inefficiency during incidents.

Recommendation: We strongly recommend that notification requirements be reconciled and streamlined to minimise duplication and enable operational teams to prioritise incident resolution. We propose that:

(i) the TCCO and ECS be amended to formally recognise the Triple Zero Custodian as a 'relevant stakeholder', ensuring the Custodian receives all Major Outage and Significant Local Outage notifications as part of existing processes;
(ii) section 13 of the TCCO be amended to require carriers and CSPs to include a clear assessment of whether an outage has a known impact on Triple Zero services in notifications, noting that many outages do not affect Triple Zero functionality; and
(iii) section 13 of the TCCO be further amended to incorporate any additional information requirements in the Triple Zero Call Failure Notification Form, rather than introducing a separate, parallel reporting stream. Consideration should also be given to distinguishing between information required during a live incident and information more appropriately provided in post-incident outcome plans under section 79 of the ECS.

[2] Vocus, '*Vocus Submission: Proposed amendments to the Telecommunications (Customer Communications for Outages) Industry Standard*' (18 February 2026).
[3] Office of Impact Analysis, *Impact Analysis* (Report, November 2024) p21 <https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Impact%20Analysis_0.pdf>.
[4] Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, '*Triple Zero Notification Protocol*' (May 2026) p1.
[5] Ibid.

B. Clarify roles and expectations for welfare checks

Vocus has identified a clear need to mature the welfare check framework to address known operational gaps. Section 28 of the ECS requires CSPs to conduct welfare checks once they become aware of a Major Outage affecting emergency call services. This means that welfare check obligations are only triggered where at least 100,000 Services in Operation (SIOs), or an entire state or territory, are impacted by an unplanned outage for more than an hour. This is a high bar and risks delaying action in circumstances where timely intervention may be critical. To strengthen public safety outcomes and improve confidence in the Triple Zero system, we recommend lowering this threshold.

Building on this, the current framework does not accurately reflect the delivery of telecommunications services across multi-layered supply chains. The CSP is not always the entity with the most direct relationship with, or visibility of, the end-user.

Recommendation: The responsibility to perform welfare checks should sit with the entity that holds the direct customer relationship and has access to end-user contact details. However, we recognise that service delivery models can be complex and varied, and there is unlikely to be a one-size-fits-all solution. For this reason, it is important that any clarification is developed in consultation with a broad cross-section of industry participants to ensure bespoke scenarios are appropriately captured. This engagement should extend beyond MNOs to include wholesalers, MVNOs and other CSPs across the supply chain.

To support this, we strongly support passage of the *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* to establish a centrally maintained CSP register. This will provide greater visibility of active CSPs and help ensure they understand and can meet their obligations.

C. Leverage existing regulatory frameworks to improve Triple Zero risk management

The consultation paper raises an important question as to whether the ACMA has sufficient powers to proactively regulate access to Triple Zero, including whether the framework should do more to promote, protect and facilitate reliable access. Vocus agrees this is a critical objective; recent reforms have largely focused on expanding notification and reporting obligations, and the next step is to focus on how existing frameworks can be better leveraged to strengthen risk management across the ecosystem.

Before introducing new obligations relating to Triple Zero risk management, we strongly recommend undertaking a more holistic review of the current legislative and regulatory landscape. There should be a clear assessment of how existing frameworks can be better leveraged and aligned. Without this, there is a real risk of layering additional requirements onto an already complex regime, without addressing underlying gaps or inefficiencies.

The telecommunications sector needs greater clarity about the role of SOCI – and by extension the Department of Home Affairs – in the management of telecommunication network outages. At present, it is unclear how the SOCI obligations are practically intended to operate alongside the Custodian, and the existing regulatory framework jointly overseen by the ACMA and the Custodian. The existing SOCI obligations already impose broad and significant risk management requirements. For example, sections 8(a) and 8(b) of the TSRMP Rules require responsible entities to minimise or eliminate the material risk of 'a stoppage or major slowdown of the relevant critical infrastructure asset's function for an unmanageable period'. The CISC guidance notes that this includes 'A systemic delay of service provision whereby a 'relevant impact' arises, for example, where an incident impacts the speed of a broadband service, thereby affecting the availability, integrity, or reliability or confidentiality of the asset such that it cannot perform its function when required.'[6]

Similarly, section 8(b) of the TSRMP Rules requires responsible entities to minimise or eliminate the material risk of 'an impairment to the relevant critical infrastructure asset's functions that prejudices the social or economic stability, or national security of, Australia.' Further, the CISC guidance notes that this includes 'Where the ability to conduct the

[6] Cyber and Infrastructure Security Centre, '*Guidance for Responsible Entities for Critical Telecommunications Assets*' (April 2025) <https://www.cisc.gov.au/resources-subsite/Documents/telecommunications-guidance.pdf>.

following is reduced: contact critical services, such as emergency services'.[7] In practice, these requirements appear to capture many of the same risks that the ECS and TCCO frameworks are designed to address.

However, there is limited practical guidance on how these regimes are intended to interact. Key questions remain unanswered – for example, whether compliance with the ECS and TCCO frameworks is expected to satisfy, in whole or in part, the requirements of the TSRMP Rules, and whether non-malicious outages (such as those caused by natural disasters) trigger additional SOCI notification expectations. Without this clarity, there is a risk of duplication, with providers diverting resources to overlapping compliance activities rather than focusing on preventing, responding to, and recovering from outages.

Recommendation: In this context, it would be premature to introduce additional Triple Zero risk management obligations without first addressing these interaction issues. A more effective approach would be to work with industry and other regulators to clearly define how the existing frameworks operate together, streamline regulatory expectations, and ensure that obligations are targeted and effective.

D. Clarify expectations about Management Plans under s80 of ECS

Vocus agrees that it is important to identify network changes that may introduce a risk to the continuity of Triple Zero services. However, in practice, the current requirements under section 80 of the ECS are difficult to apply.

Recommendation: A more practical approach would be to adopt a risk-based notification framework, where carriers notify the ACMA and/or the Custodian of changes that present a material risk of an unplanned Triple Zero outage. This would better align with how change management is undertaken in practice.

Further, the current expectation to notify up to six months in advance should be reduced. A shorter, more practical timeframe – like the 22-business day consultation period under the SOCI telecommunications notification framework – would provide regulators with sufficient oversight while remaining operationally achievable.[8]

[7] Ibid.
[8] Critical Infrastructure Security Centre, *Telecommunications Guidance* (n.d.) <https://www.cisc.gov.au/resources-subsite/Documents/telecommunications-guidance.pdf>.

Questions for comment

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?

The overarching principle informing the legislative and regulatory framework should be establishing trust in the Triple Zero ecosystem. This includes trust between telcos and the communities they serve, as well as between industry and the Custodian.

Vocus recommends delineating the roles of the ACMA and the Custodian to reduce duplication and improve trusted communication sharing with the Custodian during outages. We strongly recommend targeted amendments to the TCPSS Act to introduce a limited-use obligation for the Custodian, modelled on the NCSC. A clearer delineation of roles, supported by practical information sharing safeguards, would help foster a more collaborative environment to support a more resilient and trusted Triple Zero ecosystem.

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?

The current legislative and regulatory framework may limit the effective adoption of new technologies for accessing Triple Zero, particularly where existing concepts are not technology neutral. Key definitions such as Major Outage and Significant Local Outage rely on thresholds tied to the number of SIOs in a geographic location, and duration. While these concepts work reasonably well for traditional fixed networks, they are increasingly difficult to apply to newer technologies, including satellite-based services, where service boundaries are less geographically defined and customer location data may not be captured in the same way.

This will be particularly important as newer technologies underpinning the Universal Outdoor Mobile Obligation play a greater role in delivering emergency service access. Vocus would welcome continued engagement with the ACMA and the Custodian to ensure the settings remain fit-for-purpose as the ecosystem evolves.

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?

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?

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?

As noted in recommendation 2(c), we need clarity on whether the SOCI TSRMP requirements are intended to extend to Triple Zero risk management. It is difficult to assess the need for new risk management obligations without first clearly defining the scope of the existing regulation.

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?

Vocus is not aware of any additional information it holds that is not already made available to ESOs and would materially improve the delivery of emergency services.

In time-critical situations, our priority is to provide the most relevant and actionable information as quickly as possible – such as customer name and address details – to support processes like enhanced welfare checks.

We respectfully suggest that any consideration of new information-sharing requirements be carefully balanced against the operational realities faced by ESOs. Introducing additional reporting obligations may increase the volume of information without necessarily improving outcomes, as ESOs must triage incoming data and rely on the most critical information to perform their roles effectively.

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?

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?

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?

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

As outlined in recommendation (1), the priority should be clearly delineating the respective roles of the ACMA as regulator and the Custodian as the end-to-end coordinator of the Triple Zero service.

In this context, we support the introduction of limited-use obligations that enable timely and trusted information sharing with the Custodian in time-sensitive situations.