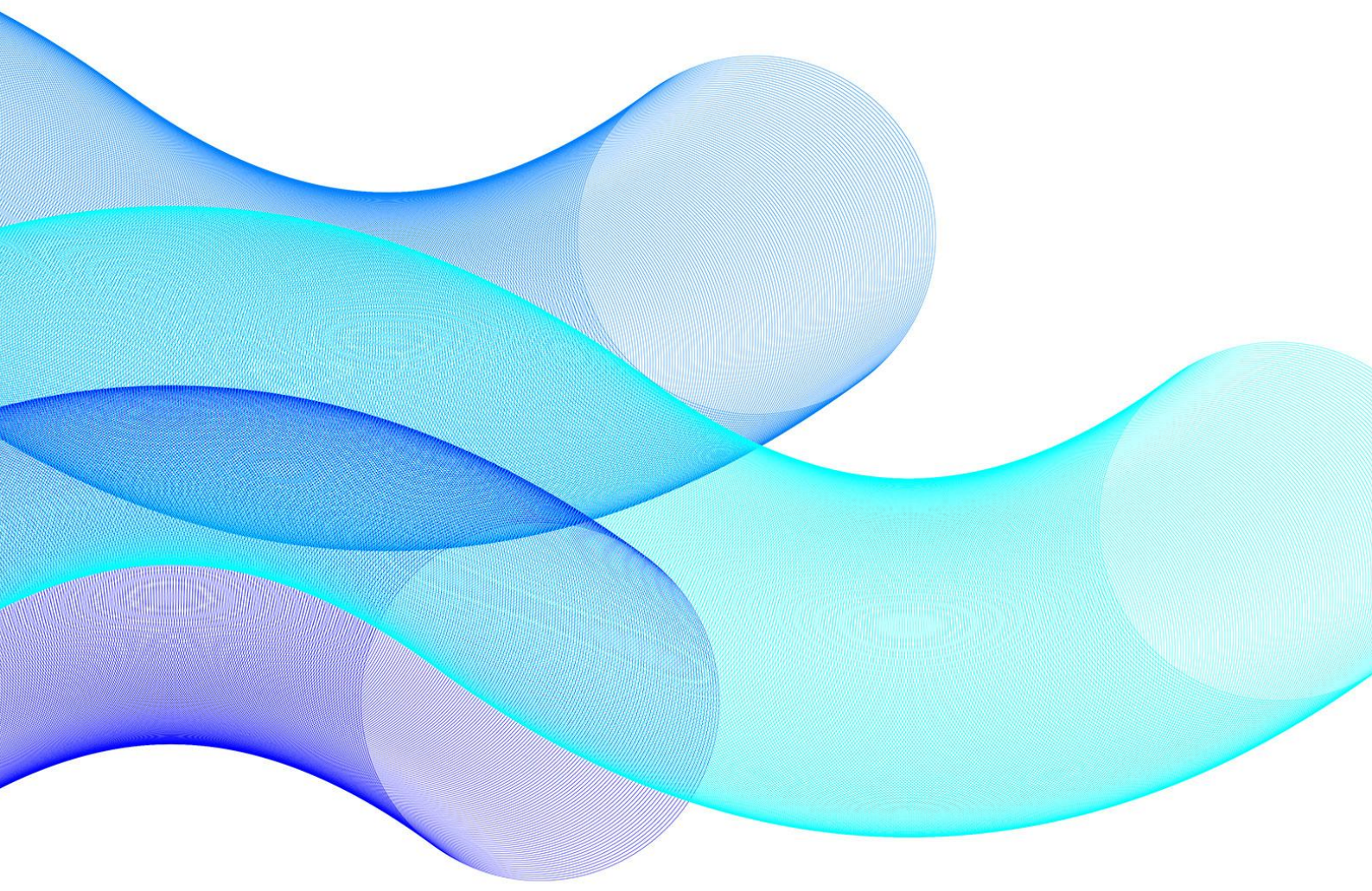
Vocus Submission

Independent Review of *Security of Critical Infrastructure Act 2018* (Cth)

19 December 2025



Vocus Group Limited | ABN 96 084 115 499 | vocus.com.au

[redacted]

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 contribute to the Independent Review of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI).

As one of Australia's largest telecommunications providers, we are committed to working collaboratively with the Independent Reviewer to strengthen the security and resilience of Australia's critical infrastructure to deliver essential services to the community. We acknowledge that the SOCI Act established world-leading protections for Australia's critical infrastructure assets and consider it to be broadly effective in achieving its objectives of enhancing security and resilience.

Vocus supports the continued maturation of the regulatory framework and has highlighted targeted areas for review and improvement:

- **Improving Harmonisation of SOCI and Telco Regulation:** Amendments to SOCI have occurred in parallel with the implementation of recommendations from the Bean Review into the Optus outage of 8 November 2023.[1] We recommend that the SOCI review take a holistic approach and consider recent changes to sector-specific regulation to ensure the overall telecommunications regulatory regime is coherent and effectively improving industry resilience.
- **Cyber Security Hazards:** We are concerned about the suitability of the Australian Signals Directorate's (ASD) Essential Eight Framework to critical telecommunications assets. We recommend reassessing the suitability of the Essential Eight and also request further clarification on data management requirements.
- **Subsea Cable Management:** We are increasingly concerned about the security of subsea cables, particularly the number of cables landing in unprotected zones. We urge Government intervention to strengthen protections and support cable operators mitigate the risk of accidental and malicious cable damage.
- **Satellite Systems:** We note the review may explore extending SOCI obligations to space technologies. Given Vocus's leadership in satellite systems, we are well-positioned to support the Independent Reviewer assess the applicability of SOCI to the space sector.

Through continued collaboration and shared ambition, Vocus looks forward to supporting the evolution of the SOCI regime and contributing to the long-term security and resilience of Australia's critical infrastructure.

[1] Australian Government Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, '*Australian Government Response to the Bean Review Final Report – Review into the Optus outage of 8 November 2023 – April 2024*' (30 April 2024) <https://www.infrastructure.gov.au/department/media/publications/australian-government-response-bean-review-final-report-review-optus-outage-8-november-2023-april>.

Improving Harmonisation of SOCI and Telco Regulation

Overview of telco regulatory landscape

Carriers and carriage service providers (CSPs) are operating in a complex regulatory landscape, comprising more than 500 legislative and regulatory instruments, of which 200 are sector specific.[2] Notably, telcos are subject to enforceable industry codes covering a range of matters, including outage management. In highly regulated sectors, effective coordination between different regulators is critical. We have seen this demonstrated across financial services, where the Commonwealth Treasury maintains a regulatory initiatives grid that provides a forward-looking view of priorities and enables coordination across multiple regulators.[3]

By comparison, the telecommunications sector has undergone significant amounts of regulatory change in recent years without centralised coordination. The amendments to the SOCI Act (including migration and expansion of TSSR) and establishment of the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP Rules) have coincided with the implementation of recommendations from the Bean Review.[4] This includes the introduction of the *Telecommunications (Customer Communications for Outages) Standard 2024* (TCCO), amendments to the *Telecommunications (Emergency Call Services) Determination 2019* (ECS), and changes to enforceable industry codes.

The ACMA is the primary regulator responsible for enforcing telco-specific legislation. In addition to the ACMA, in October 2025, the *Telecommunications Legislation Amendment (Triple Zero Custodian and Emergency Calling Powers) Act 2025* (Cth) amended the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) (TCPSS) to establish the Triple Zero Custodian (Custodian). The Custodian is empowered '*with oversight and overarching responsibility for the efficient functioning of the Triple Zero ecosystem, including monitoring the end-to-end performance of the ecosystem.*'[5] This includes powers to direct the ACMA to take certain actions.

To date, there has not been a holistic review of how these regulatory developments interact with each other. We encourage this review to holistically consider telco-specific legislation and the SOCI Act when assessing whether the current regulatory regime effectively strengthens the security and resilience of the sector. As outlined below, there are several opportunities to improve harmonisation across these regulatory frameworks.

Clarity needed on TSRMP and network outage legislation.

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 newly established Custodian, and the existing regulatory framework jointly overseen by the ACMA and the Custodian.

Under section 8(a) of the TSRMP Rules, responsible entities must 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 following is reduced: contact critical services, such as emergency services'.* [7]

These obligations appear to overlap with telecommunications specific legislation administered by the ACMA. In particular, the TCCO establishes a notification framework whereby carriers and CSPs are obligated to notify and

---

[2] ACMA, '*Improving telco communications to stakeholders during outages: Impact analysis'* (November 2024) <https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Impact%20Analysis_0.pdf>.
[3] Australian Government Treasury, '*Regulatory Initiatives Grid – December 2024'* (18 December 2024) <https://treasury.gov.au/publication/regulatory-initiatives-grid-december-2024>.
[4] Australian Government Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (n 1).
[5] The Parliament of the Commonwealth of Australia, '*Explanatory Memorandum – Telecommunications Legislation Amendment (Triple Zero Custodian and Emergency Calling Powers) Bill 2025'* (October 2025) <https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r7379_ems_d459aaec-ae11-4bfa-aa29-f40abd4589fc/upload_pdf/JC016824.pdf;fileType=application%2Fpdf>.
[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>.
[7] Ibid.

communicate with other providers, the public, end-users and government and regulatory stakeholders during the following types of outages:

(1) **Major Outage:** A major outage is when there is an unplanned adverse impact to a telco network supplying carriage services to end-users, which:
- results in an end-user being unable to establish and maintain a carriage service; and
- affects, or is likely to affect:
  - 100,000 or more services in operation; or
  - all carriage services supplied using the network in a state or territory; and
- is expected to be, or is, longer than 60 minutes.

(2) **Significant Local Outages:** A significant local outage is when there is an unplanned adverse impact to a telco network supplying carriage services to end-users, which:
- results in an end-user being unable to establish and maintain a relevant carriage service; and
- is not a major outage; and
- affects or is likely to affect:
  - 250 or more services in operation in remote Australia that is expected to last for 3 or more hours
  - 1,000 or more services in operation in regional Australia that is expected to last for 6 or more hours.[8]

If a Major Outage or Significant Local Outage affects the carriage of emergency calls, the ECS imposes additional notification obligations to communicate with Emergency Service Organisations (ESOs). The ECS also establishes comprehensive requirements governing the handling of emergency calls, including change management processes for changes that may impact the carriage of emergency calls, camp-on and wilting functionality, and welfare checks in cases where 000 calls fail.

There have been significant challenges in implementing the Major Outage and Significant Local Outage requirements. Importantly, the legislative definition of Major Outages and Significant Local Outages is assessed by number of services affected in a specific location and expected duration. Not all services in operation have an associated location, such as satellite services or voice SIP trunks, and it is acknowledged across industry that it is not technically feasible to implement certain TCCO requirements.[9] For reference, the initial impact assessment for TCCO forecast $117M in industry expenditure to implement the Major Outage Requirements. There was no financial impact assessment conducted for Significant Local Outages.[10]

Further, on 8 December 2025 the Minister for Communications issued *Telecommunications (Customer Communications for Outages Industry Standard Amendment) Direction 2025* (Direction). This requires the ACMA to amend the TCCO to impose a requirement on carriers and some CSPs to maintain outage registers on their website by 30 June 2026. While transparency is important, the imposition of additional real-time register updates risks diverting critical resources away from network management and outage resolution. As Vocus noted in our submission to the Department of Communications dated 24 November 2025, it is essential to assess the operational impact of any new outage regulations to balance notification with the risk of further diverting critical resources away from outage resolution and preventing recurrence.

The telco sector needs practical guidance on the interaction between TSRMP, TCCO, ECS and related industry codes. For example, does compliance with the ECS and TCCO satisfy, in whole or in part, the requirements of sections 8(a) and (b) of the TSRMP? Does the Department of Home Affairs expect notification of network outages with non-malicious causes (such as natural disasters)?[11] Without clarity, there is a risk of duplicative regulatory obligations consuming resources that should be directed towards preventing, responding, and recovering from network outages.

By contrast, there is a much clearer regulatory approach in the financial services sector. Critical banking, superannuation and insurance assets are not required to maintain SOCI risk management plans because they are regulated under sector-specific legislation, including the Australian Prudential Regulation Authority's (APRA) CPS 230 and 234. This approach provides clarify and avoids duplication. We strongly recommend that this review consider how

[8] See section 5, TCCO for definitions of Major Outage and Significant Local Outage.
[9] For example, see Telstra, '*Telstra submission – Environment and Communications References Committee inquiry into the Triple Zero service outage*' (25 November 2025) p16 <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/TripleZero48P/Submissions>.
[10] ACMA (n 3).
[11] For reference, please see guidance on outage notifications – ACMA, '*Rules for significant and major outages*' (18 September 2025) <https://www.acma.gov.au/rules-significant-and-major-outages>.

the telecommunications sector can be transitioned to a similar model, minimising the uncertainty around the intended operation of sector-specific legislation alongside SOCI.

There are potentially conflicting information-sharing regimes under SOCI and telco legislation.
The amended TCPSS Act enables the Custodian to compel the disclosure of information about emergency call service (ECS) outage events. It is unclear how these disclosures interact with the 'Protected Information' regime under SOCI. For example, the Custodian may compel the disclosure (without limitation) '*information relating to infrastructure affected by or related to the ECS outage event*'[12] and '*data on network performance and management before, during and after the ECS outage event*'.[13] While this information may constitute 'Protected Information', the amended TCPSS Act enables this information to be used and disclosed to a broad range of stakeholders in varying circumstances. The telco sector urgently needs guidance to confirm that compliance with Custodian information disclosures will not inadvertently breach SOCI requirements.

We also note that there are no safe harbour provisions under telco legislation. In the event of a cyber incident – within the remit of SOCI – adjacent legislation provides a clear mechanism to share information with Government. The *Cyber Security Act 2024* (Cth) establishes safe harbour protections through 'limited use' provisions, enabling organisations to voluntarily and confidentially share information with the National Cyber Security Coordinator (NCSC). The NCSC can then coordinate a whole-of-government response with the Department of Home Affairs. There is no equivalent regime between the Custodian and the ACMA. This creates a difficult and potentially conflicting situation if telcos are expected to disclose information under both SOCI and TCCO/ECS during network outages, as they may be forced to navigate two different information-sharing frameworks with different 'limited use' protections.

Cyber Security Hazards

The applicability of the Essential Eight framework for critical telco assets should be reconsidered.
We are concerned about the effectiveness of leveraging of the Essential Eight framework to minimise or eliminate the cyber security hazards for critical telco assets. The TSRMP Rules require telcos to adopt ISO27001, Essential Eight, NIST CSF, Cybersecurity Capability Maturity Model (CCMM) or the AESCSF Framework by October 2026. However, unlike the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules), the TSRMP Rules impose additional maturity requirements.

By October 2027, responsible entities must demonstrate maturity level two against Essential Eight, CCMM, or the AESCSF Framework. Importantly, both the CCMM and AESCSF are energy-sector frameworks, which in practice pushes telcos towards the Essential Eight. We acknowledge that the TSRMP rules permit adoption of an 'equivalent framework'[14], however, industry urgently needs further guidance on what this allows. The Essential Eight was designed to protect Microsoft Windows-based information technology networks and does not have a clear application to operational technology and/or telecommunications networks.[15]

This creates uncertainty about whether hybridisation with other frameworks (including NIST CSF and/or ISO27001) is necessary to fill gaps, and risks fostering a compliance-driven culture rather than threat-led risk mitigation. We recommend clearer guidance on how Essential Eight assessments should be scoped for telco assets and reconsideration of the exclusion of other widely adopted cyber frameworks.

Industry needs clearer guidance on data management expectations.
It has been difficult to implement specific data security requirements in practice. The telecommunications industry would benefit from clearer guidance on CISC's expectations on how responsible entities should minimise or eliminate the material risk of '*the storage, transmission or processing of information relevant to the operation of relevant critical infrastructure outside Australia.*'.[16] The current CISC guidance notes that '*operating critical telecommunications assets outside of Australia to provide a service in Australia exposes the service to potential interference risks and legislative regimes under which data sovereignty cannot be guaranteed.*'[17] Given the global nature of telecommunications supply chains and expansion of international hyper scalers, industry would benefit from clearer guardrails as to what constitutes acceptable risk management practices.

---

[12] TCPSS Act, section 151A(3)(f).
[13] Ibid, section 151A(3)(g).
[14] TSRMP Rules, section 11(5).
[15] Australian Signals Directorate, '*Essential Eight explained*' (27 November 2023) <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-explained>.
[16] TSRMP Rules, section 8(e).
[17] Cyber and Infrastructure Security Centre (n 6).

Further, the 2024 amendments to the SOCI Act introduced the concept of secondary 'data storage systems' which constitute part of critical infrastructure assets.[18] The current definition of 'data storage systems' appears to broadly capture IT networks, including a wide range of business support systems. Industry would benefit from guidance on whether IT networks are broadly expected to form part of critical infrastructure assets. Clearer boundaries would support entities appropriately scope SOCI programs to ensure material risks are appropriately managed.

Subsea cable management

The review of the SOCI Act should give serious consideration to the security and resilience of subsea cable infrastructure. Vocus owns and operates a growing network of subsea cables spanning nearly 15,000 kilometres and actively partners with global hyper scalers to build and leverage strategic cable investments. These assets are critical to Australia's digital economy, carrying over 99% of the nation's international internet traffic. The protection of subsea cables is therefore central to both Australia's economic future and its national security posture.

With the increasing number of cable systems landing in unprotected zones, it is imperative that the Government treat subsea cables as critical infrastructure in the national interest. This requires the application of appropriate measures to protect, monitor, and enforce the integrity of these assets. While current Cable Protection Zone (CPZ) restrictions provide a passive layer of defence, they are insufficient on their own. Active policing and enforcement will be essential to mitigate risks from both accidental damage and malicious interference.

We have previously recommended that the ACMA exercise its authority to declare additional CPZs in Darwin, Port Hedland, Maroochydore, and Christmas Island.[19] These locations are vital to Australia's connectivity with the Indo-Pacific and northern regions. Furthermore, ACMA and/or the Government should assume the cost of CPZ applications, recognising that the protection of subsea cables is a matter of national strategic importance.

Since the introduction of Schedule 3A of the *Telecommunications Act 1997* (Cth) in 2005, the number of subsea cables landing in Australia has more than doubled. Today, uninterrupted access to secure, high-capacity connectivity is a cornerstone of Australia's national resilience. The SOCI Act review must ensure that subsea cables are afforded the same level of protection and regulatory clarity as other critical infrastructure assets, to safeguard Australia's digital economy and national security for the future.

Satellite systems

Vocus understands that the Independent Reviewer may consider extending the SOCI framework to impose obligations on the owners and operators of space technologies. Given Vocus's leadership in Low Earth Orbit (LEO) satellite technology and our strategic investments in transformative space infrastructure, we are well-positioned to support the Independent Reviewer's assessment of this evolving domain. We also advocate for flexible, principles-based frameworks that allow operators to identify and manage the specific components of their assets that are most sensitive to operational resilience and national security.

For further information, please contact:

[redacted]

[18] SOCI Act, section 9(7).
[19] Vocus, '*Vocus submission – Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy*' (29 August 2025) <https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-horizon-2-of-2023-2030-australian-cyber-security-strategy>.