merillot

Submission

to the

Consultation on subordinate legislation to the *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018*

Version 1

Issued February 12th, 2024

Executive Summary

This submission responds to the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules) consultation and highlights key regulatory concerns that require revision to ensure a proportionate, risk-based, and effective approach to cybersecurity.

The proposed rules apply indiscriminate compliance obligations to all licensed telecommunications carriers, without considering their actual risk exposure or infrastructure control. Similarly, carriage service providers (CSPs) exceeding 20,000 active services are captured under full compliance obligations, despite many relying on upstream carriers for infrastructure management. These broad classifications misallocate security resources, impose unnecessary regulatory burdens, and create compliance duplication with existing regulatory frameworks such as the Telecommunications Sector Security Reforms (TSSR).

A number of critical issues are identified in this submission, including:

- Overly broad classification of carrier-owned infrastructure as critical, resulting in onerous security obligations for low-risk entities.
- An arbitrary service limit for CSP classification, requiring 20,000+ active services providers to comply with full SOCI obligations, without assessing actual security risk.
- Duplication with TSSR obligations, creating redundant compliance and reporting burdens for carriers already subject to national security obligations.
- Disproportionate incident reporting requirements, mandating the reporting of minor operational events without a clear materiality threshold, which diverts resources from genuine threats.
- Data sovereignty and storage restrictions, placing significant regulatory scrutiny on offshore storage without recognising existing cloud security frameworks or providing clear compliance pathways.
- Overly broad supply chain security obligations, requiring carriers and CSPs to assess and mitigate risks from all major suppliers, without distinguishing between high-risk and low-risk vendors.

To address these issues, Merillot recommends the following key reforms:

- Implement a risk-based classification model that differentiates between high-risk and low-risk infrastructure and CSPs.
- Refine the 20,000 active services threshold to introduce risk-based CSP classification criteria.
- Align TSRMP with TSSR obligations, ensuring a single, consolidated compliance framework to prevent duplication.
- Introduce tiered incident reporting obligations, with clear materiality thresholds to focus regulatory attention on significant cybersecurity risks.
- Clarify data storage rules, either explicitly restricting offshore storage or permitting certified international cloud providers to comply with SOCI obligations.
- Establish a risk-based supply chain framework, ensuring security obligations apply only to suppliers with access to critical infrastructure.

These recommendations will ensure that cybersecurity regulations are effective, proportionate, and strengthen national security while avoiding unnecessary compliance burdens on low-risk carriers, CSPs, and suppliers.

TABLE OF CONTENTS

1.0 Introduction

This submission responds to the consultation on the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules). These rules impose indiscriminate security and compliance obligations on all licensed telecommunications carriers. The rules, in their current form, do not considering the actual risk exposure or infrastructure control of those carriers. Similarly, the rules impose the same compliance requirements on carriage service providers, albeit with an exemption for those with fewer than 20,000 active services.

While securing critical telecommunications assets is essential, the current blanket approach misallocates resources, imposes unnecessary regulatory burdens on low-risk carriers, and duplicates existing security obligations under the Telecommunications Sector Security Reforms (TSSR).

Merillot recommends a more targeted approach, with proportional compliance framework to ensure national security objectives are met efficiently without unduly burdening smaller or wholesale-dependent carriers.

2.0 Security of Critical Infrastructure (Application) Amendment (Critical Telecommunications Assets) Rules 2024

2.1 Blanket Classification of All Carrier-Owned Infrastructure as Critical

The TSRMP Rules automatically classify all telecommunications carrier assets as 'critical infrastructure', subjecting all carriers to onerous security and reporting obligations, regardless of their size, infrastructure type, or customer base.

Unlike CSPs—where only those exceeding 20,000 active services are classified as critical—carriers are captured without any risk threshold or exclusion criteria.

This approach fails to differentiate between major national infrastructure (e.g., backbone networks, submarine cables) and regional or smaller carriers with no direct government or critical industry exposure.

Recommendations:

1. *Implement a risk-based classification model where only carriers owning or operating critical national infrastructure are captured.*
2. *Define critical telecommunications assets based on ownership of critical backbone, interconnect or submarine cables.*
3. *Exclude all carriers not captured by this definition in full from SOCI obligations, based on their low risk.*

3.0 Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules)

3.1 Insufficient service limit for Carriage Service Provider capture

The TSRMP Rules set an arbitrary threshold of 20,000 active services to classify a carriage service provider (CSP) as critical infrastructure. This approach fails to account for the actual security risks posed by different providers and instead applies a one-size-fits-all regulatory burden. A CSP exceeding this limit is immediately subject to the full suite of SOCI obligations, regardless of whether its services support critical government, defence, or essential industry operations.

This threshold lacks a clear risk-based justification. Many CSPs exceeding 20,000 services do not directly interface with end-users in a way that would constitute national security risk. Additionally, there is no distinction between providers with full network control versus those operating as resellers or virtual operators reliant on upstream carriers. Consequently, the rules risk misallocating security resources and compliance costs to providers who do not meaningfully contribute to critical telecommunications infrastructure.

Often a CSP will deliver services utilising an upstream carrier in full or in part. That upstream carrier would also be captured by the draft rules, creating a double reporting burden.

A more effective approach would be to refine the criteria for CSP capture by considering not just service volume, but also infrastructure ownership, interconnection significance, and service provision to government or critical industries. A CSP offering services to general consumers without direct involvement in backbone or interconnect operations should not be subject to the same regulatory requirements as a provider with extensive national infrastructure. Furthermore, alignment with carrier classification rules is essential to ensure consistency and proportionality in the regulatory framework.

To address these issues, the government should reassess the 20,000 active services threshold and introduce risk-based criteria that evaluate the actual security impact of a CSP. Exemptions should be introduced for low-risk CSPs that do not own or operate infrastructure critical to national security, allowing regulatory focus to remain on entities that present genuine risks. Without such refinements, the TSRMP Rules risk imposing unnecessary burdens that do not enhance security outcomes while creating inequities within the telecommunications sector.

Recommendations:

4. *Reassess the 20,000 active services threshold to introduce risk-based criteria that evaluate actual security impact rather than arbitrary service counts*
5. *Apply differentiated treatment based on infrastructure ownership, interconnectivity with other networks, and the provision of services to critical industries or government entities.*
6. *Exempt low-risk CSPs from SOCI compliance in full if they do not own or operate infrastructure critical to national security.*
7. *Align the classification criteria for CSPs with those suggested in prior recommendations for carriers, ensuring consistency and proportionality in the regulatory framework*

3.2 Duplication with Existing Telecommunications Security Reforms (TSSR)

The TSSR framework under the Telecommunications Act 1997 already mandates strong security obligations for carriers and CSPs, including:

- Preventing unauthorised network access (Section 313(1A)).
- Ensuring effective control over infrastructure (Section 313(1B)).
- Assisting national security efforts (Section 313(3)).

The TSRMP Rules add another layer of compliance without aligning with, consolidating or replacing TSSR reporting obligations.

Carriers will need to comply with two parallel security frameworks covering the same infrastructure, creating costly administrative duplication.

Recommendation

Recommendations:

8. *Clearly define the interaction between TSRMP and TSSR, ensuring regulatory obligations do not overlap.*
9. *Establish a single, consolidated compliance reporting mechanism to avoid dual reporting for the same or similar security controls.*
10. *Streamline compliance so carriers can submit one report covering both TSRMP and TSSR obligations.*

3.3 Lack of Proportionality in Incident Reporting Requirements

The TSRMP Rules require all carriers to report a wide range of security incidents and changes, regardless of their scale, impact, or relevance to national security. The broad and indiscriminate definition of what constitutes a "reportable" incident forces carriers to submit reports on events that may be routine operational issues rather than genuine security concerns.

This approach creates an unnecessary administrative burden, diverting limited security resources away from actual threat mitigation. The lack of a clear materiality threshold means that minor operational disruptions, such as localised service outages or attempted but unsuccessful cyber intrusions, must be reported alongside major cyber incidents with national security implications. This results in regulatory noise, making it harder for agencies to prioritise genuine threats and undermining the effectiveness of security oversight.

Additionally, the current framework does not account for risk tiers within the telecommunications industry. Small and medium-sized carriers, who may have minimal exposure to national security risks, are subjected to the same stringent reporting requirements as major backbone network operators. This fails to recognise proportionality in security risk management and places an unnecessary compliance burden on low-risk entities.

Recommendations:

11. *Introduce tiered reporting obligations, ensuring only incidents with a genuine national security impact are subject to mandatory reporting.*
12. *Implement clear materiality thresholds, reducing unnecessary reporting on low-risk operational events.*
13. *Establish a simplified reporting pathway for minor incidents, ensuring regulatory focus remains on significant threats.*

3.4 Overreach in Data Storage and Sovereignty Requirements

The TSRMP Rules introduce onerous compliance obligations regarding the storage and processing of business-critical data, creating uncertainty and operational burdens for telecommunications carriers. While they do not explicitly mandate that all critical data be stored within Australia, they impose significant regulatory scrutiny over offshore data storage and transmission, effectively limiting carrier flexibility in choosing secure, cost-effective cloud and data storage solutions.

The Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Amendment (Data Storage Systems) Rules 2024 extends SOCI compliance requirements to data storage systems, treating them as part of a critical infrastructure asset if they support telecommunications networks.

- Section 4(3) states that a data storage system that meets the requirements under subsection 9(7) of the Act is considered part of a critical infrastructure asset, bringing storage providers under direct SOCI regulatory oversight.

- Section 6(f) identifies risks to the availability, integrity, reliability, or confidentiality of a data storage system holding business critical data as a security concern requiring mandatory risk mitigation.

The TSRMP Rules introduce notification requirements for offshore data storage:

- Section 15 requires carriers to notify the Secretary of any changes to the way business critical data is stored or processed, including if it is transmitted or stored outside of Australia.
- Section 8(e) states that the storage, transmission, or processing of information relevant to the operation of a critical telecommunications asset outside of Australia is a material risk requiring regulatory assessment.

Recommendations:

14. *If the intent is to limit offshore data storage, state this clearly to remove doubt and uncertainty about compliance.*
15. *Recognise existing security measures and frameworks implemented by trusted cloud providers, eliminating redundant regulatory barriers*

3.5 Overly Broad Supply Chain Security Obligations

The TSRMP Rules introduce broad supply chain security obligations. The definition of “major supplier” is so broad that it captures a huge range of potential suppliers and is vague enough that many carriers or CSPs will have to develop their own definition.

Under Section 12(1)(a)(v), responsible entities must assess, minimise, or eliminate material risks arising from major suppliers, even when those suppliers do not have direct access to core infrastructure. The rules fail to differentiate between high-risk and low-risk suppliers. While "major suppliers" are defined as vendors that significantly influence the security of a critical telecommunications asset, the rules impose this blanket compliance requirements on all major suppliers, regardless of their actual impact on national security. A definition that clearly specifies the level of access or impact a supplier has on critical infrastructure would provide more practical guidance and reduce unnecessary compliance burdens.

Section 12(1)(a)(v) of rules requires carriers or CSPs to:

> *“as far as it is reasonably practicable to do so – minimise or eliminate the following material risks:*
>
> *…*
>
> *(v) arising from major suppliers”*

This appears to capture any risk from a major supplier. This could require carriers and CSPs to undertake significant compliance actions on a vast range of risks from a wide range of suppliers. This approach is unlikely to drive effective security outcomes and may instead encourage superficial, compliance-driven measures that focus on meeting regulatory requirements rather than genuine risk mitigation.

Recommendations:

16. *Introduce a risk-based classification for suppliers to differentiate between high-risk and low-risk vendors based on access to critical infrastructure.*
17. *Clarify the definition of "major supplier" to specify which suppliers have a material impact on telecommunications security.*

Appendix A – List of Recommendations

This section lists the recommendations made throughout the document.

Number	Recommendation
1	Implement a risk-based classification model where only carriers owning or operating critical national infrastructure are captured.
2	Define critical telecommunications assets based on ownership of critical backbone, interconnect or submarine cables.
3	Exclude all carriers not captured by this definition in full from SOCI obligations, based on their low risk.
4	Reassess the 20,000 active services threshold to introduce risk-based criteria that evaluate actual security impact rather than arbitrary service counts
5	Apply differentiated treatment based on infrastructure ownership, interconnectivity with other networks, and the provision of services to critical industries or government entities.
6	Exempt low-risk CSPs from SOCI compliance in full if they do not own or operate infrastructure critical to national security.
7	Align the classification criteria for CSPs with those suggested in prior recommendations for carriers, ensuring consistency and proportionality in the regulatory framework.
8	8Clearly define the interaction between TSRMP and TSSR, ensuring regulatory obligations do not overlap.
9	Establish a single, consolidated compliance reporting mechanism to avoid dual reporting for the same or similar security controls.
10	Streamline compliance so carriers can submit one report covering both TSRMP and TSSR obligations.
11	Introduce tiered reporting obligations, ensuring only incidents with a genuine national security impact are subject to mandatory reporting.
12	Implement clear materiality thresholds, reducing unnecessary reporting on low-risk operational events.
13	Establish a simplified reporting pathway for minor incidents, ensuring regulatory focus remains on significant threats.
14	If the intent is to limit offshore data storage, state this clearly to remove doubt and uncertainty about compliance.
15	Recognise existing security measures and frameworks implemented by trusted cloud providers, eliminating redundant regulatory barriers
16	Introduce a risk-based classification for suppliers to differentiate between high-risk and low-risk vendors based on access to critical infrastructure.
17	Clarify the definition of "major supplier" to specify which suppliers have a material impact on telecommunications security.