Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).

brightwave

Michael Ryan
Managing Director

GPO Box 104
Brisbane, QLD 4001

February 11th, 2025

To Whom It May Concern,

RE: Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).

Brightwave Pty Ltd is a licensed telecommunications carrier under the Telecommunications Act 1997 (Cth), as such, falls under the scope of the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules). These rules impose significant compliance obligations on all carriers. In their current draft, they provide no specific provision for exemption (although the underlying act does provide broad authority to provide exemption), regardless of operational risk or infrastructure significance.

Overly Broad Definition of Critical Telecommunications Assets

The rules automatically classify all carrier-owned assets as critical telecommunications infrastructure, regardless of their impact on national security or operational scale. Unlike carriage service providers (CSPs), where a 20,000 active service threshold determines inclusion, all carriers are captured without distinction. We suggest that a 20,000 active service threshold is also low, given the high compliance burden.

Disproportionate Compliance Burden on Lower-Risk Carriers

The lack of a risk-based approach means that carriers must comply with all security obligations, including:

- The Critical Infrastructure Risk Management Program (CIRMP).
- Mandatory cybersecurity maturity compliance.
- Incident reporting and personnel security measures.

These requirements apply uniformly, creating unnecessary regulatory burden for smaller carriers that may operate small networks of little national significance.

Lack of Flexibility in Cybersecurity Compliance Requirements

Carriers are required to comply with multiple cybersecurity frameworks without clear differentiation in implementation complexity.
While the Essential Eight Maturity Model (ASD) provides a clear, practical baseline, the inclusion of ISO/IEC 27001:2015, NIST CSF, and the US DoE C2M2 introduces unnecessary complexity.
A single, streamlined security compliance pathway should be defined, ensuring proportional and achievable standards.

Recommendations

1. Adopt a Risk-Based "Scope-In" Approach

Rather than assuming all carriers operate critical infrastructure, the rules should define which carrier assets are essential for national security.
Criteria for classification should include:

- Ownership of national backbone, interconnect, or submarine cable infrastructure.
- Supply of services to government, defence, or critical industries.
- Size-based thresholds aligned with CSP classifications.
- Carriers that do not meet these criteria should not be automatically classified as critical telecommunications infrastructure.
-

2. Establish a Tiered Cybersecurity Compliance Framework

Define minimum baseline cybersecurity requirements using the Essential Eight Maturity Model (Maturity Level 1) as the default standard.
Allow higher-tier compliance (ISO 27001, NIST CSF, C2M2) only for high-risk carriers that manage interconnect or backbone infrastructure.
Provide transition periods for implementation, ensuring realistic compliance timelines.
Clarify Exemptions and Reduce Redundancy with Existing ACMA/TSSR Obligations

3. Ensure alignment between TSRMP and the Telecommunications Sector Security

The Telecommunications Sector Security Reforms (TSSR) and the Telecommunications Act 1997 already impose security obligations on carriers and CSPs regarding foreign ownership, security risk notifications, and supply chain risks. The introduction of TSRMP, without proper alignment, creates unnecessary duplication in compliance requirements.
To ensure a cohesive regulatory framework that does not impose redundant or conflicting obligations, the TSRMP Rules should:

- Clarify how TSRMP obligations interact with TSSR requirements and avoid requiring carriers to comply with two overlapping regulatory regimes for the same security objectives.
- Consolidate reporting obligations, ensuring that cybersecurity incidents, risk management programs, and asset registrations are handled through a single regulatory mechanism, rather than requiring separate compliance pathways for TSRMP and TSSR.

Conclusion

The current blanket classification of all carriers as critical infrastructure is unnecessarily broad and places disproportionate compliance obligations on lower-risk operators. A scope-in model, risk-based classification, and tiered compliance approach would ensure that critical infrastructure security obligations are targeted and effective, without placing excessive regulatory burden on all carriers.

We welcome the opportunity to engage further in this consultation and provide industry insights into a more balanced and effective regulatory framework.

Kind Regards,

Michael Ryan