Connected Australia Pty Ltd
GPO Box 104
Brisbane, QLD 4000

Cyber and Infrastructure Security Centre
Department of Home Affairs

February 12th, 2024

To the SOCI Consultation Team,

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

At Connected Australia, we're all about fast, reliable internet without the corporate nonsense. So, when we see rules that make no sense, we call them out. The Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules) are a regulatory overreach that heaps unnecessary burdens on carriage service providers like us without a clear link to actual risk reduction. It's regulation for the sake of regulation, and that's something Australia's internet market doesn't need.

The Issues We're Calling Out

1. **Blanket Classification of All Carriers as Critical Infrastructure – Overkill Alert**
   The TSRMP Rules automatically label all licensed carriers as critical infrastructure, regardless of size, risk profile, or operational impact. Unlike CSPs, which must exceed a 20,000 active services threshold, all carriers get lumped into the same regulatory bucket. The result? Small and regional players like us are stuck jumping through unnecessary compliance hoops. Here's what's wrong with this approach:
   - It fails to differentiate between major national infrastructure and smaller carriers with smaller networks of much lower criticality.
   - It forces unnecessary security compliance on businesses that don't actually run critical infrastructure.
   - It creates disproportionate compliance burdens that stifle competition.
   - The under 20,000 exemption for CSP's is too low, and CSP's in this range may not actually operate much infrastructure.

2. **Regulatory Copy-Paste - Overlapping with Existing TSSR Rules**
   The telecommunications sector already operates under the Telecommunications Sector Security Reforms (TSSR), which mandate security obligations under the Telecommunications Act 1997. TSRMP is essentially a duplication exercise with:
   - No clear distinction between TSRMP and TSSR reporting obligations.
   - No streamlined compliance mechanism, creating double the paperwork.
   - No real benefit in terms of security improvement—just more red tape.

3. **Unrealistic Cybersecurity Compliance Requirements – What about the small guys?**
   The TSRMP Rules enforce a one-size-fits-all cybersecurity approach, demanding compliance with frameworks designed for massive enterprises:
   - **ISO/IEC 27001:2015** – Heavy-duty enterprise security framework requiring excessive documentation.
   - **Essential Eight Maturity Model (ASD)** – A practical but rigid model designed for large-scale security programs.

Connected Australia Pty Ltd
GPO Box 104
Brisbane, QLD 4000

- **NIST Cybersecurity Framework (USA), C2M2 (US DoE), AESCSF (AEMO)** – International and sector-specific frameworks that make zero sense for smaller carriers.
- No clear pathway to **right-sizing compliance** for smaller operators—forcing us to meet standards designed for critical backbone providers.

4. **Smart Device Security Compliance – Shifting the Burden to Carriers**
   The **Security Standards for Smart Devices Rules 2024** make carriers responsible for ensuring that all network-connected devices (e.g., modems, routers) meet government security standards. This creates:
   - Compliance headaches when vendors fall short.
   - Supply chain issues if critical equipment is deemed non-compliant.
   - Additional costs that hit smaller carriers the hardest.
   - Completely misses the point that the vendor should have the burden of compliance for the equipment that they sell.

5. **Supply Chain & Vendor Oversight Madness**
   - The TSRMP rules demand that we take full accountability for our entire supply chain's security practices. This is a nightmare for small carriers (and any carrier that doesn't manufacture their own hardware.)
   - No clear **liability boundaries** when vendors don't meet compliance standards.
   - The burden of ensuring international suppliers meet local security standards falls entirely on carriers, despite limited leverage over global manufacturers.

6. **Over-the-Top Cyber Incident Reporting & CIRB Oversight**
   - The Cyber Incident Review Board (CIRB) Rules 2024 require carriers to report incidents and undergo government-led reviews.
   - Minor security incidents could trigger resource-intensive reviews, draining time and money from actual service delivery.

What Needs to Change

1. **Adopt a Risk-Based Classification Model**
   - Critical infrastructure **should be defined based on actual risk**, not just a license type.
   - Classification should consider:
     - Whether a carrier owns backbone/interconnect infrastructure.
     - Whether they provide services to government/defence.
     - A reasonable service threshold (e.g., more than the 20,000+ active services which is already applied to CSPs).
   - Low-risk carriers should be excluded from unnecessary compliance.

2. **Fix the TSRMP-TSSR Overlap**
   - Clearly define the relationship between TSRMP and TSSR to eliminate redundancy.
   - Create a **single reporting mechanism** covering both obligations.
   - Cut the compliance red tape—two frameworks shouldn't exist for the same infrastructure.

3. **Introduce a Scalable Cybersecurity Compliance Framework**
   - Implement a **realistic transition period** for compliance as the periods outlined in the draft rules are not realistic for small carriers.

4. **Fix Supply Chain Compliance Expectations**

Connected Australia Pty Ltd
GPO Box 104
Brisbane, QLD 4000

- Define vendor responsibility—don't push **global supply chain risks** onto small carriers.
- Allow for **risk-based vendor oversight**, not blanket liability.
- Clarify whether **hardware vendors or carriers** are ultimately responsible for compliance.

5. **Reform CIRB's Role and Reporting Burden**
   - Limit mandatory CIRB reviews to **high-risk cybersecurity events**.

Final Word: Keep It Proportionate
The TSRMP Rules, as they stand, are overkill for smaller carriers like Connected Australia. We're all for strong security and protecting Australia's digital backbone, but let's apply **common sense**. Not all carriers are the same, and regulation should reflect **actual risk**, not just a blanket rulebook.

We look forward to continued discussions on a more balanced, risk-based approach that secures critical networks without stifling competition and innovation.

Sincerely,

Mark Frost
Operations