On Q Communications
GPO Box 104
Brisbane QLD 4001

Ph: 1300 651 641
Fax: 1300 364 660

Wednesday, February 12th, 2025

Cyber and Infrastructure Security Centre
Department of Home Affairs

Submission on the Security of Critical Infrastructure (Telecommunications) Rules 2024

To Whom It May Concern:

At On Q Communications, we take security seriously—it's the backbone of our business and our commitment to customers. However, the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024 (TSRMP Rules), as currently drafted, create significant regulatory burdens for Carriage Service Providers (CSPs) without differentiating based on actual operational impact, infrastructure type, or national security relevance.

As a CSP our business operates under a fundamentally different model from those carriers owning and managing core backbone infrastructure. Despite this, the TSRMP Rules apply broad, one-size-fits-all security requirements to CSPs that exceed 20,000 active services, creating unjustified compliance costs and obligations.

A major concern with the TSRMP Rules is the misclassification of Carriage Service Providers (CSPs) as Critical Infrastructure solely based on service volume. Unlike licensed carriers, CSPs do not control critical backbone networks or interconnection points, yet they are subject to the same stringent security requirements. Applying identical obligations to both licensed carriers and CSPs disregards the fundamental differences in their operations and creates unnecessary compliance burdens. The 20,000-service threshold used to determine whether a CSP falls under these rules is arbitrary and does not accurately reflect network significance or security risk. The classification should consider the nature of services provided, geographic risk factors, and actual network exposure rather than an overly simplistic service count.

Another critical issue is the duplication of existing telecommunications security requirements. The Telecommunications Sector Security Reforms (TSSR) already impose strict security obligations on CSPs under the Telecommunications Act 1997. Rather than creating a streamlined framework, the TSRMP Rules introduce overlapping compliance requirements without a clear mechanism for integration. This redundancy forces CSPs to navigate multiple regulatory processes, adding administrative complexity without clear security benefits.

Additionally, the compliance model outlined in the TSRMP Rules is both inefficient and costly. CSPs are required to adhere to complex security frameworks, such as ISO 27001, NIST CSF, Essential Eight, C2M2, and AESCSF. For small CSP's this will be a challenge. The rules fail to distinguish between small, regional CSPs and

those managing high-risk interconnect or backbone networks, resulting in disproportionate compliance costs for lower-risk providers. It also fails to recognise that the CSP's typically provide services over an upstream carrier's infrastructure, who presumably also must comply to the TSRMP rules. This duplication, lack of scalability and flexibility ultimately places unnecessary financial and operational strain on CSP's like On Q Communications.

To ensure the rules effectively enhance security without imposing undue burdens, a more practical and proportionate approach should be adopted instead of a blanket classification. CSPs should be evaluated based on their actual infrastructure control and service impact, rather than an arbitrary service volume. Key factors that should guide classification include ownership of interconnect, backbone, or submarine cable infrastructure, the provision of services to government or defence, and the extent to which network operations contribute to national resilience. This infrastructure-focused approach would better reflect real-world security implications rather than applying a broad, one-size-fits-all threshold.

The TSRMP Rules should be aligned with existing TSSR obligations to prevent regulatory duplication. A single, consolidated security compliance framework would allow CSPs to meet their obligations efficiently and effectively, rather than being forced to comply with two overlapping security regimes. Without this alignment, CSPs will continue to experience regulatory inefficiencies that divert resources away from actual security enhancements.

Security is critical, but excessive regulation does not necessarily lead to better security outcomes. The TSRMP Rules must acknowledge the operational differences between CSPs and licensed carriers to ensure a fair, effective, and balanced security framework. We urge the Department to adopt a more practical classification system based on infrastructure control and service impact, streamline TSRMP with existing TSSR regulations, and introduce a scalable compliance model that reflects actual security needs. These adjustments will ensure that security obligations remain meaningful and effective, while avoiding unnecessary regulatory burdens on CSPs like On Q Communications.

We welcome further consultation and appreciate the opportunity to provide feedback.

Regards,

Andrew Edington
Chief Technology Officer