Tasmanian Networks Pty Ltd
ABN 24 167 357 299
PO Box 606, Moonah, TAS, 7009

13 February 2026

Brendan Dowling
Deputy Secretary Critical Infrastructure and Protective Security
Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

Dear Brendan

Re: Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules

As the operator of Tasmania's electricity transmission and distribution networks, TasNetworks welcomes the opportunity to provide feedback to the Department of Home Affairs (the Department) in response to the consultation paper regarding proposed amendments to Australia's Critical Infrastructure Risk Management Program Rules (CIRMP Rules).

TasNetworks recognises the increasing security risks facing Australia's critical infrastructure and, in principle, supports strengthening the obligations on entities responsible for critical electricity assets. However, we hold reservations about aspects of the reforms' design, particularly the proposed implementation timeframes and the cost implications arising from both the compressed schedule and the technical complexities of the required uplifts.

As an economically regulated network business, the revenue that TasNetworks is permitted by the Australian Energy Regulator to recover from customers is set every five years. TasNetworks is currently in the second year of a regulatory period that concludes in 2029. The allowances set in 2024 provide for expenditure to address cyber security risks and comply with the *Security of Critical Infrastructure Act 2018* and the CIRMP rules as they were at the time of TasNetworks' last revenue proposal.

With a proposed implementation period of only 18 months, requiring compliance with the upgraded CIRMP obligations by 30 June 2028, TasNetworks is not funded in its current regulatory period for the uplift in risk management practices being proposed in the consultation paper. The scale and complexity of these uplifts will require significant investment by TasNetworks in both new and upgraded systems and network assets.

As this funding is not included in TasNetworks' existing allowance, recovery of the cost of complying with the updated CIRMP Rules would require a separate regulatory determination process. This introduces timing, uncertainty and evidentiary risk for the business. If full cost recovery is not achieved, TasNetworks may need to make trade-offs between CIRMP-related activities and other resilience investments planned for the current regulatory period. This risks unintended consequences, including delays in replacing near end-of-life assets that manage

Tasmanian Networks Pty Ltd
ABN 24 167 357 299
PO Box 606, Moonah, TAS, 7009

reliability and failure risk, with potential implications for network availability, which the proposed CIRMP reforms are intended to support.

Even with the requisite funding, for TasNetworks the 2028 compliance deadlines are also not considered achievable, given the scale and complexity of the (in some cases) transformational change required to deliver the enhanced measures the Department is seeking to implement. This is particularly the case in relation to some of TasNetworks' legacy operational technology systems that are used to monitor and control network assets and devices. In TasNetworks' view, the proposed uplifts involve a degree of change and a level of cost that would normally be delivered by network service providers across multiple regulatory control periods, with any capital investment to be recovered over the life of the assets.

The concurrent introduction of multiple complex obligations, without clear prioritisation, limits network operators' ability to focus on the controls that offer the greatest security benefits. This is likely to stretch limited resources and financial capacity to upgrade systems and assets, increasing delivery risk.

TasNetworks considers the proposed CIRMP reforms introduce both technical and regulatory duplication. The proposed amendments involve material overlap between the enhanced CIRMP obligations and the requirements of other frameworks, such as the Australian Energy Sector Cyber Security Framework. This overlap is likely to give rise to administrative burden, stakeholder confusion and the duplication of compliance reporting and assurance activities, diverting effort from the delivery of genuine security uplifts.

Lastly, the proposed requirement for responsible entities to manage risks from "vendors of concern" is likely to be complex and resource intensive to implement. The term is not defined in the consultation paper, creating uncertainty about scope and compliance expectations. TasNetworks also notes that in some parts of the supply chain, supplier markets are concentrated and alternative vendors may be limited, which could make strict exclusion approaches operationally challenging.

TasNetworks thanks the Department for the opportunity to comment on the consultation paper and would welcome further engagement with the Department as the CIRMP reforms progress. To discuss the views expressed in this submission please contact Alex Burk, Leader Regulation, at [redacted]

Yours faithfully

[redacted]

Marthinus Le Roux
Head of Regulation