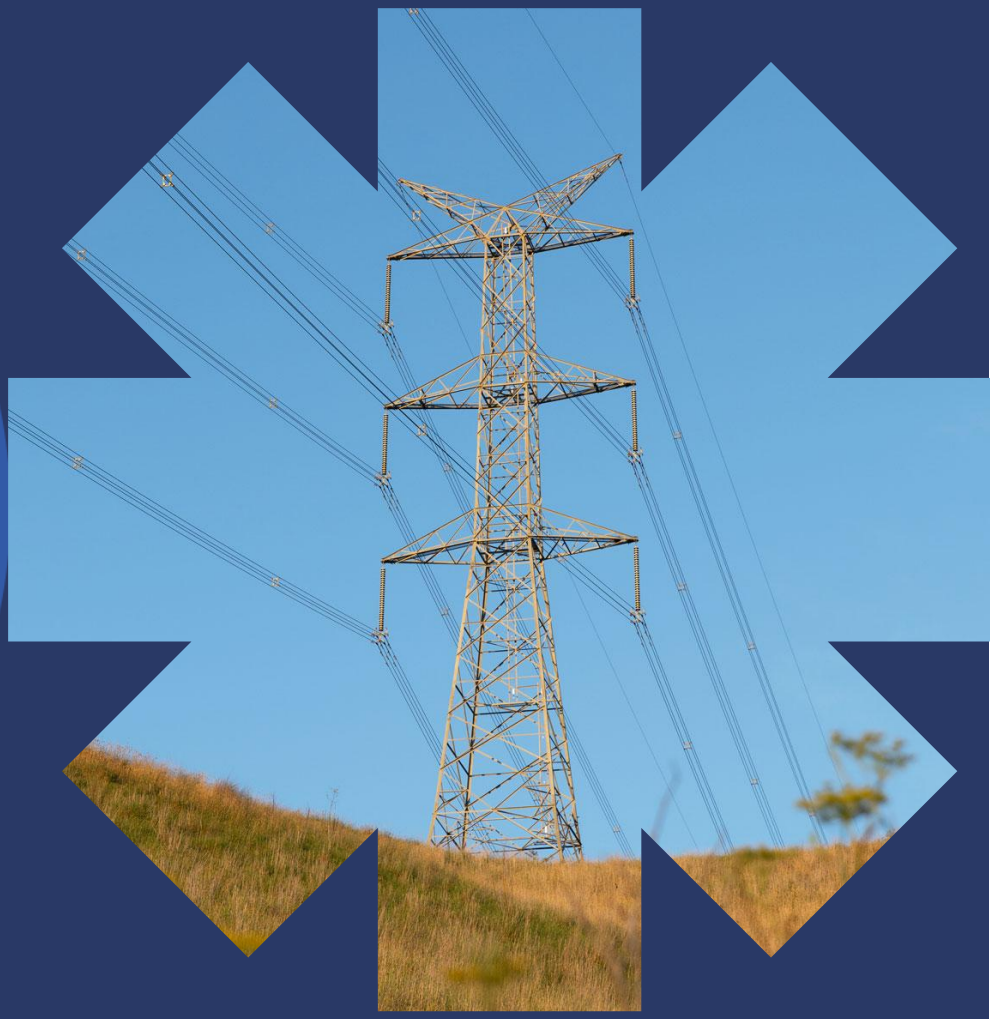
AusNet



Physical security business case

AusNet 2027-32 TRR Revised Proposal

Monday, 7 September 2026

Table of contents

1. Executive summary

This business case sets out AusNet's proposed physical security program for transmission sites, developed in response to a changing threat environment and strengthened obligations under the Security of Critical Infrastructure Act and associated Critical Infrastructure Risk Management Program requirements. AusNet's electricity transmission network is registered as critical infrastructure, and the proposed program supports the implementation of reasonably practicable measures to manage material physical security risks across critical components of the network.

The need for investment is supported by AusNet's Security Risk Assessments, which assess criticality, threat and vulnerability in accordance with recognised security risk management standards and industry guidance, including HB 167:2006, ISO 31000, ENA DOC 015-2022, the Protective Security Policy Framework and ASIO T4 Technical Notes. These assessments identify credible physical security threats, including vandalism, theft, malicious intrusion, sabotage and politically motivated violence, and assess the effectiveness of existing controls across terminal stations and other critical infrastructure sites.

AusNet's approach is risk-based and proportionate. Sites have been classified by criticality to ensure that higher-risk and more strategically important assets receive a higher level of protection, while lower-criticality assets receive controls that are targeted to the risks they face. The program focuses on improving layered security outcomes across deterrence, detection, delay, response and recovery, including through investments in fencing, gates, CCTV, access control, lighting, signage, vegetation management and protection of buildings and sub-components.

[SOCI ACT PROTECTED]

Table 1 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2. Introduction

2.1. Timeline of notable changes to SOCI Act and subordinate legislation

There is growing recognition of the role of government policy to address threats to Australian critical infrastructure assets that are increasingly interconnected and complex. Critical infrastructure is fundamental to Australia's social and economic prosperity, national security and defence. Disruptions can have consequences well beyond the affected asset because of interdependencies across sectors. Changing threat environments have led to commensurate changes in regulatory requirements, and increased policy intervention reflects the need for stronger partnerships between government and industry, alongside the shift towards imposing positive obligations on responsible entities to manage increasing risk.

The *Security of Critical Infrastructure Act 2019* (Cth) (SOCI Act)came into force in 2018 and began as a regime focused on visibility of ownership and control.[1] Under this Act, legal obligations are outlined for entities that own, operate or have direct interests in critical infrastructure assets. The SOCI Act also defines each class of critical infrastructure asset, with each critical infrastructure asset including multiple parts which function together as a system or network. AusNet's electricity transmission system meets the definition of Critical Infrastructure Asset under the SOCI Act.

Subsequently, the Security of Critical Infrastructure (Critical infrastructure risk management plan) Rules 2023 (CIRMP Rules) were introduced. These rules set out the obligations and specific requirements for how responsible entities must protect critical assets in the electricity transmission network and comply with the SOCI Act.

Under these rules, prescriptive requirements are set out for how responsible entities are required to identify, assess, mitigate, and assure material security risks. This includes developing a critical infrastructure risk management plan (CIRMP) that identifies and manages 'material risks' of 'hazards' that could have a 'relevant impact' on a critical infrastructure asset. This involves identifying hazards and risks applicable, considering the impact if risk was to eventuate, and implementing mitigation strategies or eliminating material risks (e.g., a physical security hazard for a physical critical component) as far as reasonably practicable. Within that framework, physical security is one of the core domains that responsible entities are expected to identify, assess and manage as part of compliance with the CIRMP obligations, set out in *Section 11 – Physical security hazards and natural hazards* of the CIRMP Rules.

In June 2026, further amendments under the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (CIRMP Amendment Rules) came into force. The changes to the CIRMP Rules were developed following the Independent Review of the SOCI Act, delivered in January 2026, which identified opportunities to strengthen Australia's critical infrastructure security framework and respond to a rapidly evolving threat environment.

The explanatory statement to the CIRMP Amendment Rules states that existing obligations require updating because the threat landscape has become more dynamic and challenging, including through state-sponsored and malicious actors, supply chain vulnerabilities, emerging technologies, espionage and foreign interference. The enhanced requirements specifically relevant to physical security are set out in *Rule 9A – Personnel hazards – enhanced requirements* and *Rule11A – Physical security hazards and natural hazards – enhanced requirements* of the CIRMP Rules; however, physical security requirements do feature across all rules.

2.2. Scope and purpose of this program

This business case only contains the proposed uplifts in expenditure required to comply with SOCI Act obligations that apply to physical security. AusNet is required to amend its physical security program, driven by the need to comply with SOCI Act requirements that address the ever-changing threat landscape. The following sections of the CIRMP

[1] Independent Review of the SOCI ACT - Final Report

Rules as amended impose obligations in relation to physical security and related areas, with an impact on AusNet's proposed program of investment in physical security:

- *Rule 9A – Personnel hazards – enhanced requirements*
- *Rule 11 – Physical security hazards and natural hazards*
- *Rule 11A – Physical security hazards and natural hazards – enhanced requirements*

[SOCI ACT PROTECTED]

The need for AusNet's physical security program is grounded in the requirement to maintain a risk management program that is tailored to the operating context and risk exposure of the relevant asset. For physical security, this involves establishing and maintaining a process to manage physical security risks for critical assets, consistent with legislative requirements. This involves identifying critical infrastructure assets, hazards and risks applicable, considering the impact if the risk was to eventuate, and mitigating or eliminating material risks as far as reasonably practicable. AusNet's physical security program reflects capital expenditure associated with the implementation of this risk management process.

Following the introduction of the CIRMP rules in 2023, AusNet held internal and industry discussions on interpretations, response and compliance timeframes. Following this, an assessment of critical components and security risk assessments occurred to influence the design of the physical security program. The imminently applicable reforms to the CIRMP rules place more specific obligations on AusNet (Section 11A), see figure below. AusNet is now proposing this program due to the formal compliance timeframes set out by the Department of Home Affairs. The program is due to commence in the next year.

Figure 1 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3. The identified need for investment across sites

3.1. Approach to Security Risk Assessments

[SOCI ACT PROTECTED]

3.2. The security threat to AusNet's critical infrastructure is increasing

[SOCI ACT PROTECTED]

3.3. The assessment of criticality ensures investment is proportionate to risk

[SOCI ACT PROTECTED]

3.4. Vulnerability is assessed so that investments address credible risks of security incidents

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 2 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 2 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 3 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 4 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 3 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

4. Options considered to address the identified need

4.1. Base case scenario

[SOCI ACT PROTECTED]

4.2. Investment options considered

[SOCI ACT PROTECTED]

5. Cost benefit methodology

[SOCI ACT PROTECTED]

Table 5 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 6 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

6. Selection of preferred option and justification

[SOCI ACT PROTECTED]

Table 7 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 4 [SOCI ACT PROTECTED]

A. Responses to the AER's Draft Decision

AER'S DRAFT DECISION ISSUES RAISED	AUSNET PROPOSED RESPONSE
AusNet did not provide building-block cost breakdowns by elements, site, and criticality	AusNet has provided the requested information in the Revised Proposal
AusNet did not provide sufficient detailed cost information to substantiate the aggregate costs proposed for Tier 2 sites.	AusNet has provided the requested information in the Revised Proposal
Some form of cost benefit assessment and risk assessment would assist in demonstrating works are reasonable and proportionate.	AusNet has submitted a cost benefit analysis and enterprise risk assessment in the Revised Proposal
AER Draft Decision accepts fencing and CCTV across Tier 1 sites	AusNet accept this outcome
For fencing and CCTV for Tier 2 sites, AusNet did not provide detailed cost build-ups.	AusNet will provide the requested information in the Revised Proposal
For Tier 3 fencing and CCTV, AusNet has not provided sufficient information. The AER also have concerns regarding the prudency of the proposed scope.	AusNet will provide further detail requested on CCTV and fencing. Additional Tier 3 age asset information is provided for assets such as fencing to demonstrate prudency
Added an access control allowance of $0.3 million, which we consider to be a prudent and efficient for this element.	AusNet accept the need for an access control allowance and the Revised Proposal contains an appropriate allowance amount
We expect evidence of a proportionate assessment of costs relative to consequences, noting material risk is lower in more remote parts of the network.	AusNet have submitted a cost benefit analysis, risk assessment and an assessment of criticality

B. Enterprise Risk Assessment – Asset Security

[SOCI ACT PROTECTED]

AusNet

AusNet

Level 31
2 Southbank Boulevard
Southbank VIC 3006

T 1300 360 795

Locked Bag 14051
Melbourne City Mail Centre
Melbourne VIC 8001

Follow us on

@AusNet.Energy
@AusNet

ausnet.com.au