AusNet

Transmission Revenue Reset

TRR (2027-32)

Managing Foreign Ownership, Control and Influence (FOCI) and Supply Chain Risks

Monday, 7 September 2026

Table of contents

Executive Summary 4

3. Context 6

1.1 New regulatory obligations 6

1.2 Current state 7

4. Needs identification 9

2.1 Identified risks with current situation 9

2.2 Risk assessment 11

2.3 Initiatives to address identified need 14

5. Options consideration 16

3.1 Options analysis 16

3.2 Assessment of options 16

3.3 Recommended option 21

Appendix A 21

Appendix B 22

Document history

DATE	VERSION	COMMENT
27/07/2026	V1.0	Initial draft business case for review
14/08/2026	V2.0	Revised business case incorporating input
26/08/2026	V3.0	Updated for final review
31/08/2026	V4.0	Final business case document

Related documents

DOCUMENT	VERSION	AUTHOR
4.2.12 AusNet - Wipro - Other Programs Cost Basis Report - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	Wipro
4.2.14 AusNet - Wipro Services Letter - 1 Sep 2026 – SOCI ACT PROTECTED	V1.0	Wipro
4.2.09 AusNet - Revised Digital NPV model - 1 Sep 2026 - SOCI ACT PROTECTED	V2.0	AusNet Services

Approvals

POSITION	DATE
Digital & Technology – Strategy, Regulatory and Partner Management	August 2026
Digital & Technology – Operations	August 2026
Digital & Technology – Cyber Security	August 2026
Digital & Technology – Architecture	August 2026
Group Operations – Supply Chain	August 2026
Transmission – Strategy and Regulation	August 2026

Executive Summary

The *Security of Critical Infrastructure Act 2018* (Cth)(**SOCI Act**) authorises the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023 (**CIRMP Rules**). Since AusNet's initial TRR Proposal, the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (**CIRMP Amendment Rules**) came into force on 10 June 2026 (see Attachment AusNet - Appendix 3G CIRMP Amendment Rules Mapping (Digital) - 1 Sep 2026 - SOCI ACT PROTECTED, for additional detail).

The CIRMP Amendment Rules introduce new requirements for Critical Infrastructure operators to identify, assess and manage risks of Foreign Ownership, Control and Influence (**FOCI**). The amended Rules reflect new information available to the Department of Home Affairs (**DoHA**) on heightened risks of compromise of supply chains and foreign interference activity. Relevantly, the CIRMP Amendment Rules require Critical Infrastructure providers such as AusNet to identify and manage risks of impairment of a critical infrastructure asset, risks of offshore unauthorised access to critical components and business critical data, and supply chain hazards. Importantly, the CIRMP Amendment Rules require AusNet to minimise or eliminate FOCI risks as far as reasonably practical.

In accordance with the CIRMP Amendment Rules, AusNet has identified two primary FOCI risks. Firstly, AusNet currently leverages digital capabilities from offshore, with teams having varying degrees of access to OT and IT systems, including access to operational systems. Secondly, AusNet relies on supply chains outside of Australia for critical infrastructure assets that may be subject to FOCI sabotage.

We assessed 4 credible options to manage the specific risk of FOCI induced sabotage from offshore actors and intentional disruption of supply chains as set out in **Table 1**. Our options assessment provides a quantitative basis to minimise or eliminate FOCI sabotage as far as reasonably practical. [SOCI ACT PROTECTED].

The preferred option based on cost-benefit analysis was Option 2, based on the highest net present value.

Table 1 – Summary of options and assessment outcomes ($'M, real 2025)

OPTION	CAPEX ($'M)	OPEX ($'M)	NPV ($'M)	PREFERRED
Option 1 – [SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]			No
Option 2 - [SOCI ACT PROTECTED]				**Yes**
Option 3 – [SOCI ACT PROTECTED]				No
Option 4 – [SOCI ACT PROTECTED]				No

Table 2 below details the proposed expenditure for the recommended Option 2.

[SOCI ACT PROTECTED].

All costs are the transmission network cost allocation, which represents a 50% allocation of AusNet total expenditure, consistent with our cost allocation methodology.

Table 2 – Annual expenditure required for managing FOCI risks ($'M, real 2025, transmission network allocation)

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Opex [SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]					
Capex [SOCI ACT PROTECTED]						
Ongoing Licences & Support Opex [SOCI ACT PROTECTED]						
Total						

3. Context

AusNet's initial Transmission Revenue Reset (**TRR**) proposal in October 2025 included prudent and efficient expenditure to meet the existing regulations under the SOCI Act, commensurate with the risk thresholds appropriate for our transmission network. Since our initial proposal, *the CIRMP Amendment Rules* came into effect from 10 June 2026.

The CIRMP Amendment Rules have material implications for how AusNet must assess risks and required mitigations for FOCI risks. Importantly, the public information provided by DoHA as part of the consultation process, the associated explanatory statements, and AusNet's direct engagement with the Department, have revealed that there is a heightened risk of FOCI induced disruption to Critical Infrastructure operations and/or sabotage to critical infrastructure. This new information was not known at the time of the initial proposal, and underpins AusNet's revised proposal.

1.1 New regulatory obligations

The SOCI Act authorises the CIRMP Rules that came into force in 2023. In June 2026 the CIRMP Amendment Rules came into force which enhance requirements for high-risk infrastructure such as AusNet's electricity assets.

The Explanatory Statement noted that the amendments respond to a more complex, challenging and continuously evolving threat landscape.

Consistent with this assessment, the amended Rules introduce additional material risks (rule 6A) which responsible entities, as part of their CIRMP, must establish and maintain processes to minimise or eliminate as far as is reasonably practicable. Specific to FOCI, the CIRMP Amendment Rules require AusNet to risk assess and manage:

- *6A (2)(b) compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI;*
- *6A (2)(c) offshore or remote access to critical components; and*
- *6A (2)(d) offshore or remote access to business-critical data.*

Rule 10A sets out enhanced CIRMP requirements that a responsible entity must comply with in relation to supply chain hazards. In relation to supply chain hazards, the CIRMP Rules as amended require:

- *10A(2) A responsible entity of a CI asset specified in subsection 4A(1) must establish and maintain a system or process in the entity's CIRMP to map their supply chain for major suppliers and critical components across their supply chains.*
- *10A(3) In accordance with subsection (2), the entity's CIRMP must:*
    - *(a) identify risks in the entity's supply chain that may affect the availability, integrity, reliability or confidentiality of critical components or compromise business critical data; and*
    - *(b) identify the maximum acceptable outage for the CI asset or any of its critical components arising from the disruption to the entity's supply chain; and*
    - *(c) as far as is reasonably practicable to do so—include measures to minimise or eliminate those risks, or mitigate the impact of an outage that exceeds the maximum acceptable outage identified in paragraph (3)(b).*
- *10A(4) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset.*
- *10A(5) The system or process outlined in subsection (4) must identify, for each existing or proposed major supplier:*
    - *(a) in relation to FOCI risks—legislative or other legal requirements to which the supplier is subject to; and*
    - *(b) restrictions, sanctions or other impediments affecting the jurisdiction to which the entity may be subject to; and*

- *(c) the access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides; and*
- *(d) the extent to which the matters in paragraphs (a), (b) and (c) together may present a material risk for the CI asset, or could exceed a maximum acceptable outage of the service or product provided by the supplier; and*
- *(e) as far as reasonably practicable to do so—steps to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.*

- *10A(6) For subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to:*
  - *(a) whether the CIRMP includes a process or system capable of identifying the matters in paragraphs (3)(a), (b) and (c) for their CI asset; and*
  - *(b) whether the CIRMP includes a process or system capable of identifying the matters in paragraphs (5)(a) to (e).*

In summary, under the CIRMP Amendment Rules, AusNet as a responsible entity must establish and maintain processes to identify FOCI and supply chain hazards that could give rise to a material risk, assess the likelihood and consequences of those risks, and implement appropriate measures to minimise or eliminate them so far as is reasonably practicable.

1.2 Current state

The CIRMP Amendment Rules have material implications for AusNet's transmission business. As detailed below, AusNet utilises digital services partners with personnel located outside of Australia who have privileged access to Operational Technology (OT) and Information Technology (IT) systems. In addition, AusNet's critical infrastructure operations depend on a globally interconnected supply chain spanning technology providers, field service partners, equipment manufacturers and specialist suppliers. While these arrangements provide access to essential capabilities, they also create dependencies on overseas suppliers, manufacturing facilities, logistics networks and support services that are increasingly exposed to geopolitical, operational and supply chain disruption risks.

Digital services delivery from outside of Australia

Over the past decade, AusNet has progressively expanded the use of offshore digital services delivery through strategic partnerships with providers such as IBM and Wipro. While most of our critical digital systems support such as SCADA are provided in Australia, our service providers have more than [SOCI ACT PROTECTED] support personnel located in India. This digital model supports 24x7 operations, provides AusNet access to specialised capabilities, and improves the cost efficiency of our technology services.

While many of these personnel perform routine support and maintenance activities, a significant proportion have privileged access to critical business and operational technology environments. Privileged access means elevated permissions that allow a user to access, control or make significant changes to critical OT and IT systems beyond those available to ordinary users. In particular, AusNet's OT systems meet the definition of a critical component under the SOCI Act being "part of the Critical Infrastructure asset, where absence of, damage to, or compromise of, the part of the asset would prevent the proper function of the asset, or could cause significant damage to the asset".

AusNet undertakes verification of pre-employment processes used by our contracted service providers. However, we cannot perform the same level of vetting as for Australian-based personnel, including using AusCheck. Additionally we note that India is not part of the [SOCI ACT PROTECTED] comprising Australia, Canada, New Zealand, the United Kingdom and the United States that form a long-standing intelligence-sharing partnership.

The breadth of access reflects the evolution of AusNet's operating model and highlights the concentration of operational, cyber security, data sovereignty and insider threat risks associated with a large offshore workforce supporting essential energy services.

AusNet's vendors and supply chains extend outside of Australia

AusNet's critical infrastructure operations depend on a globally interconnected supply chain comprising technology providers, service delivery partners, field service partners, equipment manufacturers and specialist suppliers.

AusNet relies on an extensive network of suppliers, including technology providers ([SOCI ACT PROTECTED]), service delivery partners ([SOCI ACT PROTECTED]), and manufacturers of critical network equipment such as transformers,

switchgear, conductors and other network assets. Many of these organisations operate globally or depend on international manufacturing, logistics and support networks. These arrangements provide access to specialised equipment, software, technical expertise and support services that are essential to network operations, but also create dependencies on overseas manufacturers, service providers, logistics networks and sub-tier suppliers that sit beyond AusNet's direct contractual relationships.

As a result, AusNet is inherently exposed to global supply chain dependencies. Many critical materials, equipment and digital services originate from international markets and rely on overseas manufacturing facilities, specialist expertise, global logistics networks and offshore support arrangements. In some cases, suppliers operate in highly concentrated markets where there are limited alternative providers, long manufacturing lead times, or proprietary technologies that cannot be readily substituted.

AusNet currently undertakes third-party risk assessments for selected suppliers, incorporating considerations such as ethics, ownership structures, country of operation and financial viability. While these activities provide a degree of oversight of direct supplier relationships, they were not designed to address the enhanced supply chain obligations introduced under the amended SOCI framework.

4. Needs identification

The purpose of this section is to outline the methodology used to identify and assess FOCI-related sabotage risks associated with: (a) personnel and service providers operating outside Australia; and (b) international supply chains. This includes an assessment of current risk exposure and the proposed mitigation initiatives to address identified risks.

As noted in Section 1.1, the CIRMP Amendment Rules require AusNet to explicitly identify, assess and manage risks from FOCI, offshore teams' remote systems access, and supply chain disruption. Consistent with this requirement, AusNet has undertaken assessment of these risks, incorporating assessment of consequences and likelihood utilising AusNet's Enterprise Risk Management Framework.

2.1 Identified risks with current situation

We have separately considered the risk scenarios of (1) the delivery of digital services using personnel located outside of Australia and (2) supply chain disruption related to overseas vendors, manufacturers and supply routes. [SOCI ACT PROTECTED]

Offshore teams providing digital services

The plausible risk scenario posed by offshore personnel providing digital services is the manipulation or sabotage of an OT or IT system leading to electricity transmission operational service disruption, release of confidential data, or disruption to business operations due to a digital systems outage. The risk arises where offshore personnel have privileged access to critical systems, creating the potential for malicious interference, unauthorised access, data exfiltration, system manipulation or sabotage that may impact the availability, integrity or reliability of critical infrastructure operations.

The likelihood of occurrence is considered greater for offshore personnel due to reduced suitability assurance, visibility, and oversight compared with Australian-based personnel. As discussed in Section 1.2, Australian vetting processes utilise strong processes such as AusCheck, and these processes cannot be implemented as robustly in locations outside of Australia. Further, for onshore resources, AusNet can more readily draw on information, guidance and threat intelligence from Australian Government security agencies. These safeguards can be more difficult to replicate for personnel outside of Australia where access to reliable information may be more limited and different legal and governmental environments may apply. Foreign service providers may be obliged by local laws to release data or provide access without Australian oversight.

AusNet assessed each offshore-delivered capability based on the level of privileged access to operational technology (OT) systems, personally identifiable information (PII) and business-critical systems. For each capability, AusNet considered the function performed, the level of access available across OT and IT environments, and the potential consequences should that access be misused, compromised or used for sabotage.

[SOCI ACT PROTECTED]

Supply chain risks

The plausible offshore supply chain risk scenario involves compromise of a critical electricity network asset, operational technology (OT) system, business system or software component. This could be through sabotage, fragmented supply chain, or interference that could lead to deliberatively defective products, substandard quality or delays. Such sabotage could occur during the design, manufacture, assembly, transport or maintenance of a product or service that supports critical infrastructure operations.

As with offshore workforce arrangements, global supply chains can increase exposure to FOCI risks due to reduced visibility and oversight across international jurisdictions. These risks may arise where critical goods, software or services are sourced, manufactured or transported through overseas locations, particularly where supply chains involve multiple parties, limited transparency or jurisdictions with elevated geopolitical or security concerns. The complexity of global supply chains can also reduce AusNet's ability to identify, assess and monitor potential malicious interference, unauthorised access or the introduction of compromised components before they enter the operating environment

AusNet currently [SOCI ACT PROTECTED] .

While third-party risk assessments are performed for selected suppliers, these activities are primarily focused on direct supplier relationships and do not provide sufficient visibility of critical supply chain dependencies or broader supplier ecosystems. Key gaps include:

[SOCI ACT PROTECTED]

2.2 Risk assessment

Consequence assessment

We identified four potential consequences that could arise from a FOCI related sabotage event involving offshore personnel arrangements or international supply chain dependencies as outlined in **Table 3**.

Table 3 – Event, description and rating of consequences

Risk Type	Event	Description	Consequence rating
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]

Likelihood assessment

Likelihood has been assessed by considering the combination of willingness, capability and opportunity. For a FOCI-related incident to occur, an insider threat actor must possess the motivation to cause harm, the capability to undertake the activity, and sufficient access to critical systems, information or services to achieve the intended outcome.

In the context of this assessment, the primary threat scenario is not opportunistic cybercrime or financially motivated ransomware activity. Rather, the focus is on malicious insiders, coerced personnel, compromised suppliers, or individuals operating under FOCI arrangements whose actions could result in sabotage, disruption of critical infrastructure, or unauthorised access to sensitive information. The likelihood assigned to each consequence reflects an assessment of the:

- attractiveness of AusNet as a critical infrastructure operator responsible for the operation of Victoria's electricity and gas networks;
- willingness of a threat actor to target that capability;
- capability required to successfully execute the activity;
- level of privileged access required; and
- opportunity for the activity to occur without prevention or detection.

In assessing likelihood, AusNet has specifically focused on the incremental risk associated with personnel and supply chain dependencies located outside Australia, compared to equivalent Australian-based arrangements. Recognising the inherent difficulty in quantifying national security and sabotage risks, the assessment has been informed by the CIRMP Amendment Rules Explanatory Statement, the ASIO Annual Threat Assessment, and

[SOCI ACT PROTECTED]

Given the challenge in assessing likelihood of FOCI risks, in our options assessment we have also undertaken sensitivity testing to evaluate the impact of alternate likelihood reductions. **Table 4** sets out the likelihood assessment.

Table 4 – Likelihood assessment

Event	FOCI likelihood rationale	Offshore / FOCI exposed likelihood	Australia - based likelihood	Incremental likelihood reduction
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Risk assessment outcome

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2.3 Initiatives to address identified need

To address the identified FOCI-related sabotage risks associated with offshore personnel arrangements and international supply chains, AusNet has identified a range of targeted initiatives designed to strengthen risk identification, assessment, monitoring and mitigation capabilities

Addressing FOCI risk with offshore personnel

[SOCI ACT PROTECTED]

Addressing FOCI risks within supply chains

To address the identified capability gaps and support compliance with the additional requirements, AusNet proposes the implementation of an integrated supplier management platform spanning the end-to-end supplier lifecycle. The platform will establish a single source of truth for supplier information, risk management activities, compliance obligations and supply chain intelligence, enabling a more comprehensive and auditable approach to managing supply chain and FOCI-related risks.

The proposed solution will deliver the following capabilities:

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Together, these capabilities will provide the governance, processes and technology required to support compliance with the Enhanced CIRMP supply chain obligations while improving visibility of supplier dependencies, concentration risks, supply chain vulnerabilities and potential disruption across AusNet's critical infrastructure supply chain. Together, these capabilities would provide the governance, processes and technology required to support compliance with the Enhanced CIRMP supply chain obligations while improving visibility of supplier dependencies, concentration risks, supply chain vulnerabilities and potential disruption scenarios across AusNet's broader supplier ecosystem.

5. Options consideration

In developing this business case, we have focused on the AER's expectations on the method and approach that should be applied to proposed non-recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019. The AER expects that networks will evidence the need and demonstrate prudency and efficiency of the investment. It is expected that options of scope and timing (to demonstrate prudency) and options for alternative implementation approaches (to demonstrate efficiency) will be evaluated. As per the AER guidelines, we have examined credible options for mitigating FOCI risks.

Importantly, the CIRMP Amendment Rules require AusNet to mitigate risks as far as is reasonably practicable. This means that while the assessed current risk level of some FOCI scenarios is below our material risk threshold, we have still actively considered options that further reduce risk and assessed "reasonably practicable" based on the outcome of net present value analysis.

3.1 Options analysis

AusNet currently faces elevated FOCI risk arising from offshore workforce arrangements and international supply chain dependencies. All options have been assessed against a "do nothing" scenario, representing the continuation of current controls and capabilities.

Four credible options have been identified and assessed, as outlined in **Table 5**.

[SOCI ACT PROTECTED]

3.2 Assessment of options

In this section, we evaluate the advantages and disadvantages of each of the three options, and set out the results of the NPV analysis. We note that expenditure in this program is 50 per cent allocated to AusNet's transmission business, consistent with our cost allocation method.

Option 1 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Option 2 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Option 3 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Option 4 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.3 Recommended option

Table 10 provides a summary of findings from our options analysis. It shows that **Option 2** is recommended as it has the highest NPV relative to the other options. This reflects that the option mitigates the most material consequences of FOCI related risks [SOCI ACT PROTECTED]

The costs of this option are 50% attributable to AusNet's transmission business and the operating expenditure has been proposed as an opex step change.

Table 10 - Options analysis summary

Criteria	Option 1	Option 2	Option 3	Option 4
Capex ($'million, real FY2025)				
Opex ($'million, real FY2025)				
NPV ($'million, real FY2025)				
Technically feasible		[SOCI ACT PROTECTED]		
Addresses identified need				
Deliverable within timeframe				
Preferred option				

[SOCI ACT PROTECTED]

Appendix A – Offshore OT digital support teams

Table 12 identifies the offshore teams that currently provide services requiring privileged access to systems supporting AusNet's Operational Technology systems, infrastructure and applications. These personnel have the ability to administer systems, modify configurations, manage user access, perform restoration activities, and access business-critical or sensitive information.

[SOCI ACT PROTECTED]

Table 12 – Teams outside of Australia with privileged access to OT systems

Appendix B – Integrated supply chain system scope

Table 13 sets out the scope of the integrated supply chain system identified in the preferred option.

Table 13 - Scope of preferred option for integrated supplier system

[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