

AusNet



Transmission Revenue Reset TRR (2027-32)

CIRMP Amendment Rules Non-Digital

Tuesday, 1 September 2026

Purpose of this document

In this document, we discuss how each obligation in the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (**CIRMP Amendment Rules**) has been addressed through the non-digital components of the Revised Proposal. In particular, we have provided a mapping of the key requirements of the CIRMP Amendment Rules to the relevant appendices, business cases, and supporting documents within our submission, to assist the AER in navigating the suite of files provided. This document should be read alongside Chapters 3 and 4 of the Revised Proposal, the Technology Documents which provide information on the digital programs which support compliance to the CIRMP Amendment Rules, and Appendix 4C.

We have also provided an indication of the enterprise-wide impact of each non-digital initiative, given that AusNet owns and operates multiple networks who may each be impacted by these initiatives. This is intended to assist the AER in identifying where initiatives relate to shared resources. However, as the proposal has been prepared primarily for the Transmission network to support the Revised Proposal, some items may refer to the Transmission requirements only, even when costs are required for other networks. Future regulatory submissions may provide further information on the requirements relating to AusNet's other networks.

Summary

The table below provides a high-level summary of how the components of the Revised Proposal address the CIRMP Amendment Rules. For clarity, references to specific rules are as included in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023 (**CIRMP Rules**), as amended by the CIRMP Amendment Rules. Further information is then provided in the sections below.

Table 1: CIRMP Amendment Rules in the Revised Proposal

CIRMP Rules	Digital programs	Non-Digital programs
6A Additional material risks – enhanced requirements	Foreign Ownership Control & Influence (FOCI) and Supply Chain digital capex & opex program	Opex step change [SOCI ACT PROTECTED]
8A Cyber & Info Security Hazards – Enhanced Requirements	Patching digital capex & opex program AI Defence digital capex & opex program - Also addressed by existing Cybersecurity program (AESCSF V2 Security Profile 3)	Opex step change [SOCI ACT PROTECTED]
8B Credential compromise hazards	N/A – addressed by existing cybersecurity program (AESCSF V2 Security Profile 3)	N/A
8C Lateral movement hazards	Critical Infrastructure (CI) Fortify digital capex & opex program	N/A
9A Personnel hazards – enhanced requirements	N/A	Physical Security capex program Opex step change [SOCI ACT PROTECTED]
10A Supply chain hazards – enhanced requirements	Foreign Ownership Control & Influence (FOCI) and Supply Chain digital capex & opex program	Opex step change [SOCI ACT PROTECTED]
11A Physical security hazards and natural hazards – enhanced requirements	N/A	Physical Security capex program Opex step change [SOCI ACT PROTECTED]

The CIRMP Amendment Rules stipulate grace periods during which the enhanced obligations do not apply to certain CI Assets. A summary table is provided below, with line items also provided in the relevant sections for easy reference.

Table 2 : CIRMP Amendment Rules Timeline for application of requirements

CIRMP Amendment Rules Requirements	Grace Period
• Section 6A • Subsection 8A(2) • Subsection 9A(2)	Period of 12 months after the commencement of the instrument ¹
• Section 8A (other than subsection 8A(2)) • Section 8B • Section 8C • Section 9A (other than subsection 9A(2)) • Section 10A • Section 11A	Period of 24 months after the commencement of the instrument ²

¹ We note that the wording “the period of [x] months after the commencement of this instrument” is included in Schedule 1 Part 5 of the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026, which amends the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023. The same wording is now included in rule 4A(6) of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023. In view of the Explanatory Statement to the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026, specifically Schedule 4, Item 5, under the heading “Grace Periods”, the reference to “commencement of this instrument” must be understood as reference to commencement of the relevant subsection, that is, the commencement of the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026.

² See FN1.

6A Additional material risks – enhanced requirements

Current state and gaps

[SOCI ACT PROTECTED]

How we assessed the efficient costs of addressing these gaps

[SOCI ACT PROTECTED]

Figure 1: Risk & Assurance team structure

[SOCI ACT PROTECTED]

CIRMP Amendment Rules timeline for application of requirements

Enhanced CIRMP Rule Requirements	Grace Period
Section 6A	Period of 12 months after the commencement of the instrument ³

Relevant supporting documents

Appendix 4C provides the options considered, the analysis of the lowest cost to comply, and the cost build up for the preferred option. Market information and previous quotes have been provided which inform the costs of the preferred and non-preferred options.

Enterprise impact

The proposed costs will drive operating expenditure only, for AusNet’s Transmission and Distribution networks.

³ See FN 1.

8A Cyber & Information Security Hazards – Enhanced Requirements

These requirements are addressed by the Digital programs. Please refer to the Technology Documents.

Note: The SOCI Program Manager role is also relevant to addressing Rule 8A but is explained only in reference to Rule 6A above for brevity.

8B Credential compromise hazards

These requirements are addressed by the Digital programs. Please refer to the Technology Documents.

8C Lateral movement hazards

These requirements are addressed by the Digital programs. Please refer to the Technology Documents.

9A Personnel hazards – enhanced requirements

Current state and gaps

[SOCI ACT PROTECTED]

How we assessed the efficient costs of addressing these gaps

[SOCI ACT PROTECTED]

Figure 2: Physical Security team structure

[SOCI ACT PROTECTED]

CIRMP Amendment Rules timeline for application of requirements

Enhanced CIRMP Rule Requirements	Grace Period
Subsection 9A(2) <i>[Personnel security - access management]</i>	Period of 12 months after the commencement of the instrument ⁴
Section 9A <i>[Personnel hazards - enhanced requirements]</i> (other than subsection 9A(2))	Period of 24 months after the commencement of the instrument ⁵

Relevant supporting documents

Appendix 4C provides the options considered, the analysis of the lowest cost to comply, and the cost build up for the preferred option. It also explains how critical worker headcount for shared functions has been attributed to the Transmission and Distribution networks.

Enterprise impact

The proposed costs will drive operating expenditure only, for AusNet's Transmission and Distribution networks.

⁴ See FN 1.

⁵ See FN 1.

10A Supply chain hazards – enhanced requirements

Current state and gaps

[SOCI ACT PROTECTED]

How we assessed the efficient costs of addressing these gaps

[SOCI ACT PROTECTED]

CIRMP Amendment Rules timeline for application of requirements

Enhanced CIRMP Rule Requirements	Grace Period
Section 10A <i>[Supply chain hazards - enhanced requirements]</i>	Period of 24 months after the commencement of the instrument ⁶

Relevant supporting documents

Appendix 4C provides the options considered, the analysis of the lowest cost to comply, and the cost build up for the preferred option. The costing of consultant costs within the options has been based on consultant quotes sourced from multiple firms.

Enterprise impact

The proposed costs will drive operating expenditure only, for AusNet’s Transmission and Distribution networks.

⁶ See FN 1.

11A Physical security hazards and natural hazards – enhanced requirements

Current state and gaps

Compliance with this obligation involves establishing and maintaining a process to manage physical security risks for Critical Infrastructure assets, consistent with legislative requirements. This involves identifying critical components, hazards and risks applicable, considering the impact if the risk was to eventuate, and mitigating or eliminating material risks as far as reasonably practicable.

[SOCI ACT PROTECTED]

How we assessed the efficient costs of addressing these gaps

AusNet's Physical Security program, which was included in the Initial Proposal and is also included in this Revised Proposal, addresses the requirements of rule 11A. 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, to address material risks to physical security as far as reasonably practicable.

[SOCI ACT PROTECTED] This options assessment recognises that a uniform security standard across all sites would not be efficient or proportionate. To support the above assessment, a cost benefit analysis and risk assessment were conducted, and have been provided alongside this submission.

The proposed investment mix is expected to deliver a material improvement in physical security, reduce exposure to material security risks, support compliance with SOCI obligations, and provide an efficient and proportionate outcome for customers.

Note: The Physical Security capital expenditure program is also relevant to addressing Rule 9A but is explained only in reference to Rule 11A here for brevity.

[SOCI ACT PROTECTED]

CIRMP Amendment Rules timeline for application of requirements

Enhanced CIRMP Rule Requirements	Grace Period
Section 11A <i>[Physical security hazards and natural hazards - enhanced requirements]</i>	Period of 24 months after the commencement of the instrument ⁷

Relevant supporting documents

A suite of Technical Documents is provided in support of the Physical Security program, including a business case, cost-benefit analyses, a criticality procedure, and a detailed cost buildup. Appendix 4C provides the options considered for [SOCI ACT PROTECTED], including the analysis of the lowest cost to comply and the cost build up for the preferred option.

⁷ See FN 1.

Enterprise impact

The Physical Security program impacts capital expenditure only, and the [SOCl ACT PROTECTED] initiative impacts operating expenditure only. The costs included in the Revised Proposal are for the Transmission network only.

Similar activities may be needed for AusNet's other networks, but detail on such activities is not provided for the purpose of this Transmission Revised Proposal submission.

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

