AusNet

Transmission Revenue Reset TRR (2027-32)

Critical Infrastructure Fortify (CI Fortify) Business Case

Monday, 7 September 2026

Table of contents

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
4.2.11 AusNet - Wipro CI Fortify Cost Basis Report - 1 Sep 2026 - CONF	V1.0	Wipro
AusNet - Wipro - Services Cost Letter - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	Wipro
AusNet - IBM - Services Cost Letter - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	IBM
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 – Architecture	August 2026
Digital & Technology – Cyber Security	August 2026
Transmission – Network Operations	August 2026
Transmission – Strategy and Regulation	August 2026

Executive Summary

AusNet operates critical electricity transmission infrastructure that underpins the reliable supply of electricity across Victoria. As a critical infrastructure operator, AusNet is a potential target for increasingly sophisticated cyber threats. While AusNet is investing to achieve Australian Energy Sector Cyber Security Framework (AESCSF) Version 2 Security Profile 3 maturity through our Cyber Security program, recent legislative changes relating to Australian critical infrastructure have introduced an additional and distinct requirement focused on operational resilience and consequence management.

Recent regulatory developments have significantly increased expectations on critical infrastructure operators to ensure the resilience of operational technology (OT) environments. In particular, the focus has shifted from protecting systems to maintaining the delivery of critical services during and after a cyber incident. Network segregation has become a key control to limit the spread of cyber threats, preserve operational capability, and enable recovery when corporate IT systems or internet connectivity are unavailable.

The Enhanced Critical Infrastructure Risk Management Program (CIRMP) Rules, introduced by the Department of Home Affairs in June 2026, establish new obligations for operators of critical infrastructure to prevent the lateral movement of cyber threats between systems and networks. Section 8C requires operators to maintain critical services during a cyber incident, isolate critical systems when necessary, and recover operations from trusted sources. A central requirement is the ability for critical OT systems to continue supporting the delivery of essential services for three months even when separated from enterprise IT systems and disconnected from the internet.

The expectations of the CIRMP Amendment Rules are based on the Australian Signals Directorate's Critical Infrastructure Fortify (CI Fortify) program, first released in October 2025 and supplemented by further guidance in July 2026. This guidance program similarly promotes a resilient operating model in which critical infrastructure services can be sustained for at least three months despite the compromise or loss of corporate IT systems and external connectivity.

Together, CI Fortify and the CIRMP Amendment Rules create a clear regulatory and security requirement to enable network segregation and operational resilience capabilities. These obligations were not in place when AusNet's original TRR proposal was developed and are not fully addressed through the existing AESCSF-aligned cyber security program alone.

[SOCI ACT PROTECTED]

Table 1 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

The investment is required to ensure AusNet can maintain critical transmission operations during a severe cyber security incident or persistent threats, meet our obligations under the CIRMP Amendment Rules, and continue to provide safe and reliable electricity services to Victorian customers. It represents a prudent and efficient response to a materially changed threat landscape and resulting regulatory expectations, through investment in operational resilience which would not be otherwise achieved through existing cyber security investment programs.

Table 2 below details the proposed $15.4m capex and $16.7m opex ($real 2025) investment for CI Fortify. All costs represent transmission network allocation, which is allocated as 50% of the total AusNet program cost as per AusNet's cost allocation methodology.

Table 2 – Summary of proposed costs for CI Fortify (Option 2) ($'million, FY25, transmission network allocation)

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Capex	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
Opex	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]
Total	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]	[SOCI ACT PROTECTED]

1. Context

Over the past ten months since AusNet's initial TRR 2027-32 regulatory proposal, there has been rapid and significant development in the obligations and expectations of critical infrastructure owners in response to cyber threats.

In October 2025 the Australian Signals Directorate (ASD) issued its Critical Infrastructure Fortify ("CI Fortify") guidelines.[1] CI Fortify was established in response to escalating threats from malicious actors targeting critical infrastructure, compromised trust with third parties, and alignment to international best practice frameworks and expectations. CI Fortify sets new resilience expectations for critical infrastructure asset operators to maintain continuity of critical operations for three months during a severe cyber security incident or other disruption.

On 10 June 2026, the Department of Home Affairs (DoHA) commenced the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (CIRMP Amendment Rules). These CIRMP Amendment Rules establish new and enhanced expectations for critical infrastructure operators beyond the existing Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023 (CIRMP Rules) that were in force at the time of AusNet's initial TRR submission.

The CIRMP Amendment Rules are consistent with the objectives of ASD's CI Fortify, specifically in relation to lateral movement of threats. These new obligations are also not captured by any other initiatives or business cases that have been proposed by AusNet. They represent 'net new' requirements.

Over the past 6 months, in developing our required actions for CI Fortify and resulting TRR Revised Proposal, AusNet has undertaken significant working group engagements with DoHA, the ASD, and the Australian Energy Market Operator (AEMO). Through these engagements AusNet has clarified the objectives and minimum expectations around CI Fortify and the need to be able to separate our information technology (IT) and operating technology (OT) systems.

On 28 July 2026, the ASD published their 'CI Fortify – Advice for isolating vital systems' guidance paper[2] which provides further clarification on how an organisation can isolate critical OT systems in response to cyber incidents or periods of increased threat. This paper is consistent with the discussions held between AusNet and ASD through 2026.

1.1. The Australian Signals Directorate's CI Fortify program and CIRMP Amendment Rules

CI Fortify requires critical infrastructure operators to strengthen cyber resilience by ensuring critical OT systems can be isolated from IT and external networks for up to three months, while maintaining critical services. Organisations must identify critical systems and isolation points, maintain accurate inventories of OT and dependent systems, and understand asset interdependencies to support effective isolation.

Operators must also be capable of rapidly rebuilding isolated systems from trusted, clean sources and restoring operations without compromising service delivery. This requires systems to be designed and tested for efficient recovery following a cyber incident.

The ASD has stated that operators must act now, as cyber threats to critical infrastructure are already being realised. Key preparations include maintaining up-to-date asset inventories, testing isolation arrangements, establishing secure offline communications, and ensuring the capability to both isolate and fully rebuild critical OT and enabling systems while continuing to provide essential services.

The CIRMP Amendment Rules set out several new and enhanced requirements for IT and OT systems that significantly increase requirements for cyber security, OT security, workforce vetting, supplier oversight, and physical security. The overall objective is to improve resilience of critical infrastructure by requiring operators to better understand their critical systems, control access to them, reduce potential cyber-attack pathways, manage supply chain dependencies, and

[1] https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/ci-fortify/ci-fortify-guidance-for-australian-critical-infrastructure-service-continuity-and-resilience

[2] CI Fortify – Advice for isolating vital systems | Cyber.gov.au

prepare for both physical and cyber disruptions. As critical infrastructure, the CIRMP Amendment Rules are applicable to AusNet's electricity transmission, electricity distribution and gas distribution networks.

A summary of the new and enhanced requirements, referring to rule numbers under the CIRMP Rules as amended, is set out below or available online[3]. Rule 8C of the CIRMP Rules as amended is the basis for implementation of the ASD's CI Fortify expectations.

- **6A Additional Material Risks**. Responsible entities must identify and manage additional risks that could significantly affect Australia's economy, society, national security or defence. This includes risks associated with foreign ownership, control or influence (FOCI), and remote or offshore access to critical systems and business-critical data.
- **8A Cyber & Information Security Hazards.** Organisations must manage cyber risks by maintaining supported and patched systems, addressing risks from obsolete technology, and assessing emerging technologies. They must also implement a recognised cyber security framework, such as ISO 27001, ASD Essential Eight, NIST CSF, AESCSF or an equivalent framework that provides a similar level of protection.
- **8B Credential Compromise Hazards.** Organisations must reduce the risk of compromised user credentials by identifying where phishing-resistant multi-factor authentication (MFA) is required, implementing MFA controls, and monitoring authentication activity. The goal is to prevent unauthorised access to critical systems and services.
- **8C Lateral Movement Hazards.** Organisations must prevent cyber attackers from moving between systems or networks after gaining access. This includes maintaining inventories of critical systems, planning for recovery and restoration, and implementing network segregation, access controls, monitoring and least-privilege principles to limit the spread and impact of incidents. Organisations must demonstrate that during network segregation events critical operational technology (OT) systems can continue to operate for a period of at least three months, and be recovered, even if information technology (IT) systems are compromised and there is no access to the internet.
- **9A Personnel Hazards.** Organisations must control access to critical assets and ensure workers with access to critical components undergo an AusCheck assessment or hold an appropriate security clearance, with ongoing monitoring of their suitability and access privileges.
- **10A Supply Chain Hazards.** Organisations must understand and manage supply chain risks by mapping critical suppliers and components, identifying potential disruptions, and assessing acceptable outage limits. They must also assess supplier risks, including foreign influence, legal obligations and the level of access or control suppliers have over the asset.
- **11A Physical Security Hazards and Natural Hazards.** Organisations must centrally manage physical security and natural hazards, identify critical sites, systems and data locations, and assess how all hazards could create physical security consequences. Appropriate controls, monitoring and response arrangements must be in place to improve resilience and recovery.

1.2. How AusNet is addressing the CIRMP Amendment Rules

AusNet has undertaken a comprehensive assessment of the impacts of the updated Critical Infrastructure Risk Management Program (CIRMP) requirements across our transmission, distribution and gas networks. This assessment has found that a number of the new requirements are already being addressed through our existing TRR 2027-32 proposal programs, including our digital resilience programs and cyber security investments aligned with the Australian Energy Sector Cyber Security Framework (AESCSF) Security Profile 3 maturity.

However, our assessment also identified several material risks and capability gaps that are not fully addressed under the current investment programs. The scope of additional investment proposed in this submission is required to address the new obligations introduced through the CIRMP Amendment Rules, which were not in existence at the time of our TRR initial proposal.

[3] Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 - Federal Register of Legislation

Importantly, AusNet's cyber security and critical infrastructure risk baseline has changed materially since development of our initial TRR submission. Over the past 12 months, engagement with DoHA, ASD, AEMO and other industry stakeholders has highlighted an increasingly sophisticated and persistent cyber threat landscape targeting critical infrastructure operators, the risks created by rapid technological change such as artificial intelligence and other advanced technologies, and a stronger regulatory focus on operational resilience, consequence management and demonstrable security outcomes. Collectively, these developments have increased AusNet's risk profile and drive the need for targeted investment beyond the programs included in our initial TRR proposal.

For each of the elements in the CIRMP Amendment Rules we have identified whether the requirements are addressed by existing programs in our initial TRR proposal, or whether new investments are required. This is reflective of our approach of clearly considering and addressing each requirement prudently and efficiently. In **Table 3** below we have summarised this mapping and provided reference to the new business cases in our TRR Revised Proposal that are required to meet 'net new' requirements.

This business case is focused on addressing the requirements of 8C Lateral Movement Hazards, through delivery of the ASD's CI Fortify expectations.

Table 3 – How AusNet is addressing the CIRMP Amendment Rules requirements

Enhanced CRIMP Rules element	New requirement	Captured in
6A Additional Material Risks	New requirement	New FOCI & Supply Chain business case and opex step change in Appendix H – CIRMP Amendment Rules (Non-Digital)
8A Cyber & Information Security Hazards	Broadly covered by AESCSF V2	Existing Cyber Security program (AESCSF V2 SP3)
	New requirements related to emerging technologies and patching are in addition to AESCSF V2	New AI For Cyber Defence and New Patching business cases
8B Credential Compromise Hazards	Already covered through AESCSF V2	Existing Cyber Security program (AESCSF V2 SP3)
8C Lateral Movement Hazards	New requirement	**New CI Fortify business case (IT/OT isolation and recovery)**
9A Personnel Hazards	New requirement	Physical Security program and opex step change in Appendix H – CIRMP Amendment Rules (Non-Digital)
10A Supply Chain Hazards	New requirement	New FOCI & Supply Chain business case and opex step change in Appendix H – CIRMP Amendment Rules (Non-Digital)
11A Physical Security Hazards and Natural Hazards	New requirement	Physical Security program and opex step change in Appendix H – CIRMP Amendment Rules (Non-Digital)

1.3. Current state of AusNet's IT and OT systems

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 1 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

1.4. Impact of IT and OT Separation

Under the ASD's CI Fortify operating model, AusNet may be required to isolate OT systems from the broader IT environment during a significant cyber event for up to 3 months. In the current architecture, this would require severing the connections between the Converged Core Network Fabric and the OT environment, as illustrated by the red dashed IT/OT separation boundary in **Figure 1**.

While this action would reduce the risk of cyber threats propagating from IT into OT systems, it would also interrupt a significant number of critical applications (described in the section below), supporting services and information flows that currently rely on shared infrastructure. Review of the current architecture identified several Mission Critical systems (AusNet's highest digital criticality level, ascribed to systems essential to maintaining core operations) that would cease functioning or experience material degradation under this separation scenario. These systems support network control, outage management, operational communications, maintenance delivery, physical security and regulatory obligations variously across electricity transmission, electricity distribution and gas distribution operations.

While AusNet would retain the ability to operate some core control systems, the loss of critical supporting services would materially impact the organisation's ability to efficiently operate, maintain and restore essential network services during a prolonged cyber isolation event (i.e., the CI Fortify 3-month duration expectation). This creates the need for investment to reduce shared dependencies and enable critical operational capabilities to continue functioning when IT and OT environments are separated.

[SOCI ACT PROTECTED]

Recognising that it is neither practical nor economic to preserve every service at its current level during an OT isolation event, nor is this the CIRMP Amendment Rules and CI Fortify expectation, we undertook a detailed assessment of the

operational impacts arising from IT/OT separation. This assessment considered the extent to which individual services could continue operating through existing business continuity plans or workarounds, operate in a degraded state with additional manual effort, require additional resourcing, or warrant investment to maintain an acceptable level of resilience.

For AusNet's electricity transmission operations, this assessment covered 6 key service areas:

- Network control
- Unplanned maintenance work
- Planned maintenance work
- Landholder and engagement communications
- Protective Security & Access Controls
- Metering

Not all transmission services would be affected in the same way. Some services would continue operating, some would operate in a degraded state, and others would cease functioning entirely. While core SCADA and control room capabilities would allow AusNet to retain basic operation of the transmission network, many supporting systems and processes would be unavailable or significantly constrained. Existing workarounds are generally designed for short-duration disruptions and would require substantial additional manual effort, reliance on point-in-time information and acceptance of increased operational, compliance and service-delivery risk if sustained for up to three months.

Table 4 summarises the key transmission capabilities affected, the associated operational impacts and the potential consequences for network visibility, outage coordination, field operations, physical security and compliance obligations. The assessment identifies areas where existing controls and workarounds may be sufficient, as well as areas that drive investment and changes to our digital systems and business continuity plans as part of the CI Fortify program.

Table 4 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

1.5. Whole of AusNet implementation and transmission network cost allocation

Due to the integrated nature of our IT and OT systems across our electricity transmission, electricity distribution and gas distribution networks, the CIRMP Amendment Rules and the impact of IT and OT separation affect all of AusNet's services.

While the consequences and risks being managed through IT / OT separation vary across our three networks, the separation capability is a common requirement. Due to the integration of our digital infrastructure and services, it is not possible to implement different approaches to isolation for each of the three networks. AusNet's approach to meet the requirements of CI Fortify is driven primarily by the needs of our electricity transmission and distribution networks.

Consistent with AusNet's Cost Allocation Methodology (CAM), investments required to deliver CI Fortify expectations for a specific network have been 100% allocated to that network. Investments that are shared across networks (such as shared OT hosting infrastructure) have been allocated 50% / 50% to AusNet's electricity transmission and distribution networks.

This TRR business case is only requesting funding for the transmission network allocated costs. The remaining required expenditure will be requested via the appropriate regulatory mechanism, i.e. a cost pass through application for electricity distribution. We note that there is a critical dependency between these funding applications; if one is not approved there will be insufficient funding to implement the proposed AusNet-wide solutions and we will be challenged to comply with the obligations set out under the CIRMP Amendment Rules.

2. Needs identification

This section sets out the obligations, risks and gaps that need to be addressed to enable AusNet to comply with the CIRMP Amendment Rules and ASD's CI Fortify expectations:

- CIRMP Rules (as amended) Section 8C Lateral movement hazards
- Design guidance from ASD and engagement with other agencies
- Application to our systems
- Risk assessment

AusNet's cyber security program and the AESCSF framework consider IT and OT systems separately and provide materially increased security to prevent access into AusNet's systems and movement within these systems. However, the need for separation of the systems to prevent lateral movement of cyber attacks is a new requirement brought about by the CIRMP Amendment Rules Section 8C and the ASD CI Fortify guidance. There are no system or practice requirements within the AESCSF V2 framework that directly require separation to mitigate lateral movement of hazards from IT to OT systems.

[SOCI ACT PROTECTED]

The ASD and AEMO have reinforced with AusNet that no matter how good our practices are, malicious actors remain a threat [SOCI ACT PROTECTED]

2.1. CIRMP Amendment Rules Section 8C

The CIRMP Amendment Rules define 'lateral movement hazards' as a new hazard vector. The Rules require AusNet, as a critical infrastructure owner, to minimise or eliminate any material risk of a lateral movement hazard occurring and mitigate the relevant impact on the critical infrastructure, so far as is reasonably practicable to do so.

Rule 8C of the CIRMP Rules as amended can be summarised as now requiring:

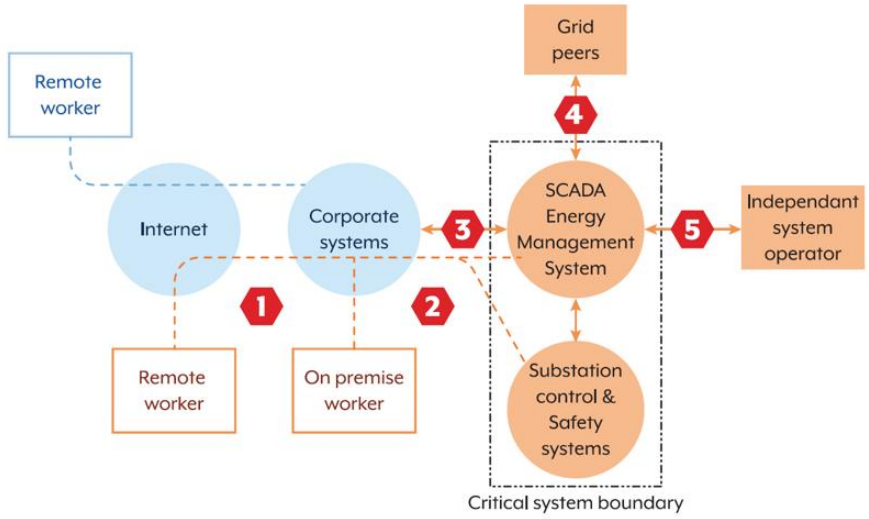
- The establishment and maintenance of recovery and resilience processes for critical systems by keeping an inventory of critical systems and their connections, enabling system recovery and restoration after incidents, maintaining asset availability during recovery, and minimising the risk and impact of lateral movement across systems.
- Network segregation as the deemed acceptable control for managing lateral movement risk, with implementation of compliant network segregation satisfying the requirement to minimise or eliminate material risks arising from lateral movement hazards.
- The implementation of key network segregation measures including separating critical systems from other systems, ensuring operational independence, maintaining critical system operations for at least three months during restoration activities, applying network access controls, monitoring and reviewing communication logs, and enforcing least-privilege access principles.
- Where full network segregation cannot be achieved, implementation of reasonable alternative controls to minimise or eliminate material risks associated with lateral movement hazards and meet the entity's broader risk management obligations.
- A demonstration of effective management of lateral movement risks by identifying relevant hazards, documenting processes to identify critical systems, dependencies and recovery requirements, and including appropriate controls to minimise or eliminate material risks to the critical infrastructure asset.

We note that since there are options for AusNet to implement full network segregation, item 4 above does not apply, and the requirement is for AusNet to implement full network segregation.

2.2. CI Fortify design principles

With the release of the CIRMP Amendment Rules and ASD's CI Fortify guidelines, AusNet has undertaken a detailed assessment of the systems, services and operational processes that would be affected by an IT/OT isolation event. This assessment considered the potential operational impacts, compliance implications and investment required to maintain critical electricity services during a cyber incident.

To support implementation of the CIRMP Amendment Rules, ASD has developed guidance outlining how critical infrastructure entities should structure their IT and OT environments to maintain critical operational services while isolating systems during a cyber event. **Figure 2** illustrates ASD's principles for critical system isolation and the need to identify, protect and maintain those systems required for the safe and reliable operation of critical infrastructure assets.



1. Disable the ability for remote workers to access OT environments (via jump hosts in intermediate non-OT systems).
2. Disable the ability for on-premises remote access to OT environments.
3. Isolate all connections between non-OT and OT environments.
4. Isolate lower priority connections between peer OT and OT environments.
5. Isolate OT environment and vital systems completely.

Figure 2 ASD's principles for critical system isolation

Through engagement with ASD and assessment of AusNet's operating environment, three broad approaches to achieving IT/OT separation were identified:

- Logical separation involves establishing logical boundaries between IT and OT environments through firewall rules, network zoning, routing controls and application reconfiguration. This approach largely retains the existing shared infrastructure architecture and relies on logical controls rather than dedicated infrastructure to isolate systems during a cyber event.
- Physical separation builds on logical separation but also introduces dedicated OT infrastructure, including servers, firewalls and network components, to remove shared dependencies between IT and OT environments. Critical systems that are currently located within the IT environment are relocated to dedicated OT infrastructure, enabling the environments to operate independently during an isolation event.
- Separation of telecommunications pathways. This will involve installing separate end devices for communications infrastructure (i.e. MPLS or DWDM units) and potentially separate telecommunications carriers would be used with separate infrastructure. This would provide complete separation and remove common points throughout the IT and OT systems. We note that these assets are already protected as part of the OT system's physical and cyber security so the risk reduction achieved is expected to be relatively low compared to the cost.

The extent of logical and physical separation can be varied to optimise cost and risk outcomes. [SOCI ACT PROTECTED]

2.3. Application to AusNet's systems

The current architecture of AusNet's IT and OT environments is shown in **Figure 3**. The architecture has evolved over time to support efficient network operations and information sharing, resulting in a high degree of integration between IT and OT systems. While this converged architecture delivers operational benefits under normal operating conditions, it creates challenges in meeting the isolation requirements of CIRMP Rules Section 8C and ASD's CI Fortify guidance.

ASD's guidance requires critical operational services to remain available during an IT/OT isolation event. Achieving this outcome is particularly complex for AusNet because many systems, applications, communications platforms and operational processes currently rely on shared infrastructure or connections between IT and OT environments.

As a result, AusNet has undertaken a detailed assessment of its system architecture to identify the changes necessary to maintain critical operational services during an isolation event. These changes can be achieved through varying degrees of logical separation, physical separation and segmentation of OT systems, resulting in different costs, risk outcomes and levels of resilience.

In assessing these necessary changes, AusNet has engaged extensively with AEMO to align on the critical operational services and secure external interfaces required to be available during a CI Fortify event in order to maintain electricity transmission system and National Electricity Market (NEM) operations. These are:

[SOCI ACT PROTECTED]

These are highlighted in **Figure 3** below.

[SOCI ACT PROTECTED]

Figure 3 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2.4. Risk assessment

Consistent with the CIRMP Amendment Rules expectation of risk-based action, AusNet has completed a risk assessment relative to the Section 8C Rules and CI Fortify guidelines. Recognising that AusNet is progressing a cyber security program to achieve AESCSF V2 SP3 maturity, the base case assumes this program has been successfully implemented and target maturity achieved. The analysis therefore assesses the risk position after existing cyber security controls and planned cyber security investments are in place.

Consequence methodology

[SOCI ACT PROTECTED]

Likelihood methodology

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Outcome

[SOCI ACT PROTECTED]

Figure 4 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3. Options consideration

We have assessed multiple options that will enable us to achieve the objectives of DoHA's CIRMP Amended Rules Section 8C and ASD's CI Fortify guidance. Consistent with the CIRMP expectation of eliminating or mitigating risks as far as is reasonably practicable, we have undertaken quantitative cost vs risk-benefit assessment to ascertain the recommended option.

As part of this assessment, we identified one option that was deemed non-credible on the basis it did not pursue compliance with the CIRMP Amended Rules. Reasoning for assessment of this option as non-credible is provided and it serves as the reference case against which other options have been assessed.

3.1. Options analysis

AusNet identified three credible options and one non-credible option to address the CIRMP Amended Rules Section 8C and ASD's CI Fortify guidance. [SOCI ACT PROTECTED]

The options were assessed against their ability to address the identified need, satisfy the requirements of the CIRMP Rules (Section 8C), and provide an efficient and prudent level of resilience for critical electricity services.

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Cost-benefit analysis was undertaken for the three credible options. The assessment considered implementation expenditure (capex and project opex), ongoing operating expenditure, and the extent to which each option addresses the identified need and improves AusNet's resilience during IT/OT isolation events. Options were assessed relative to the baseline of no further investment.

The benefits of each option were assessed using a consistent set of assumptions and reflect the extent to which each option improves compliance with the CIRMP Amendment Rules, reduces operational risk and maintains critical electricity services during an IT/OT isolation event. The preferred option was selected based on its ability to deliver the greatest overall resilience and operational benefit relative to its cost.

The assessed risk likelihood reduction for each option is detailed in **Table 5** below. [SOCI ACT PROTECTED]

Table 5 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.2. Assessment of options

In this section, we describe each option, evaluate the advantages and disadvantages of each, and set out the results of the risk assessment and cost benefit analysis.

3.2.1. Option 1 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 5 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 6 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 6 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.2.2. Option 2 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 7 - [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 7 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 8 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED

]

3.2.3. Option 3 [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 9 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 8 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Figure 10 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.3. Recommended option

Our analysis identified the need for investment to meet the requirements of the CIRMP Rules as amended, Section 8C, and the ASD's CI Fortify guidance. [SOCI ACT PROTECTED]

Table 9 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 10 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 11 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Appendix A – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Appendix B – [SOCI ACT PROTECTED]

[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