AusNet

Transmission Revenue Reset TRR (2027-32)

AI for Cyber Defence Business Case

Monday, 7 September 2026

Table of contents

Document history

DATE	VERSION	COMMENT
28/07/2026	V1.0	Initial draft business case for review
17/08/2026	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
4.2.09 AusNet - Revised Digital NPV model - 1 Sep 2026 - SOCI ACT PROTECTED	V2.0	AusNet Services
4.2.15 AusNet - Microsoft - AI Security Response - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	AusNet Services
4.2.16 AusNet - IBM - AI Security Response - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	AusNet Services

Approvals

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

Executive summary

Artificial intelligence (AI) is rapidly changing the cyber security landscape for critical infrastructure operators. It is enabling malicious actors to identify vulnerabilities, automate attacks and exploit weaknesses at a speed and scale not previously possible. Electricity networks are a high-value target because of the potential consequences of disruption to essential services, access to customer data and impact on public safety. Recent guidance from Australian Government agencies highlights that critical infrastructure operators should take proactive steps to manage both the risks created by use of AI and the risks arising from AI-enabled cyber attacks.

AusNet is increasingly reliant on digital technologies to operate and manage our electricity network. At the same time, AI capabilities are becoming embedded in enterprise software, operational technologies and third-party services. This creates a new category of cyber risk that is not fully addressed by our existing AESCSF Version 2 cyber security program, or our new proposed CI Fortify and Patching programs. These risks fall into two broad categories. First, AI is increasing the capability, scale and sophistication of cyber threat actors, resulting in a higher volume of more effective attacks. Second, the growing adoption of AI introduces new organisational risks, including unauthorised use, data exposure, compromised information or model integrity, unsafe outcomes, and increasing reliance on third-party AI products and services.

The need to invest

[SOCI ACT PROTECTED]

The need for investment is also driven by the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (**CIRMP Amendment Rules**), which require critical infrastructure entities to identify, assess and manage risks arising from emerging technologies, including AI. These requirements extend beyond traditional cyber security controls and create an obligation for AusNet to implement both governance measures and practical capabilities to defend against AI-enabled threats.

Options assessment

[SOCI ACT PROTECTED]

Our assessment, summarised in **Table 1** below, found that Option 2 provides the minimum prudent and efficient level of investment required to address the identified risks, comply with the CIRMP Amendment Rules and reduce residual risk to below AusNet's material risk threshold. While Option 3 provides additional risk reduction benefits, the assessment found that the increased cost is not justified by the incremental reduction in risk achieved.

[SOCI ACT PROTECTED]

Table 1 – Proposed AI for Cyber Defence expenditure (Option 2) ($m, real 2025, transmission network cost allocation)

Cost item	RY2028	RY2029	RY2030	RY2031	RY2032	Total
Capex	[SOCI ACT PROTECTED]					
Project Implementation Opex ("propex", non-recurrent opex)						
Ongoing Licences, Support and Token Opex (recurrent opex)						
Total						

1. Context

Artificial intelligence (AI) is changing the cyber security landscape faster than most technology shifts experienced by critical infrastructure operators and, for electricity networks, AI presents a significant threat. Critical infrastructure is a key target of cyber attacks due to the essential nature of its services and the extensive customer and sensitive data held. The Australian Cyber Security Centre (**ACSC**) found recently that about 25 per cent of reported cyber security incidents involved Australia's critical infrastructure, and that the electricity sector constitutes 30% of the reported cyber security incidents in critical infrastructure for 2023-2024.

Recent guidance from the ACSC highlights that highly capable AI models are increasing the scale, speed and sophistication of cyber attacks. The capabilities of the new frontier AI models have been repeatedly demonstrated this year to be able to find existing but previously unknown vulnerabilities and then quickly use these to attack systems. This includes complex chain attacks that link multiple system attributes together to enable full takeover.

In addition to increasing the sophistication of cyber attacks, AI is creating new organisational risks as it becomes embedded within enterprise software, operational technologies and third-party services. These risks include unauthorised AI use, data exposure, compromised model integrity, unsafe outcomes and increased reliance on third-party AI providers, requiring dedicated governance, monitoring and control capabilities beyond those used for traditional IT and OT systems.

Threats are increasing

The capabilities of advanced or "frontier" AI models are evolving rapidly. Although malicious use of AI does not necessarily create entirely new classes of vulnerabilities, it can significantly accelerate the identification, analysis and exploitation of existing weaknesses. The ACSC notes that successive generations of frontier models are becoming increasingly proficient at reading, reasoning about and manipulating software code, reducing the expertise, effort and time traditionally required to discover and exploit vulnerabilities. This has recently (August 2026) been reinforced by both the Australian Prudential Regulation Authority (**APRA**) and the Australian Securities and Investments Commission (**ASIC**) who stated that organisations need to be prepared for the speed, scale and sophistication of cyber threats.[1]

The widespread availability of AI is lowering the cost and effort required to conduct cyber-attacks, enabling increasingly sophisticated attacks to be executed at greater scale and velocity.[2,3] Organisations that don't re-evaluate and improve their defences, enabled by AI, will remain vulnerable to these AI-enabled cyber threats.

Existing cyber defence capabilities were designed to detect, investigate and respond to threats at a human-manageable speed and scale. Specialised teams, established workflows and conventional automation remain essential, however their reliance on manual analysis, static rules and sequential processes limit their ability to keep pace with the growing volume and complexity of cyber threats. This impedes the timely prioritisation of risks, investigation of threats and maintenance of effective defensive coverage.[4]

These developments demonstrate that AI capabilities are advancing more quickly than cyber security governance and risk management frameworks, such as AESCSF. Therefore, it is imperative for AusNet to adapt its controls beyond baseline framework requirements to respond to threats not yet fully contemplated by those frameworks. Investment in AI-enabled cyber defence is required to ensure AusNet can detect, investigate and respond to threats at the speed, scale and sophistication of an increasingly AI-enabled threat environment.

AI introduces a new technology risk surface

As AI capabilities become increasingly embedded within business workflows, enterprise applications, operational systems and third-party services, AusNet must ensure these technologies are deployed, governed and monitored appropriately. Without appropriate governance and safeguards, AI adoption can introduce new risks.

Key areas where and how these risks can occur include:

[1] https://www.apra.gov.au/news-and-publications/apra-and-asic-warn-frontier-ai-awareness-must-turn-action
[2] https://www.dragos.com/blog/ai-assisted-ics-attack-water-utility
[3] https://www.computing.co.uk/news-analysis/2026/fortibleed-campaign-exposes-scale-automated-cyberattacks
[4] https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/opportunities-for-ai-in-cyber-defence

- Limited visibility of AI adoption across applications, vendor platforms and embedded product features.
- Unapproved or unmanaged use of AI ("Shadow AI") by employees outside approved governance and security controls.
- Inappropriate access to sensitive information by AI tools, agents or third-party AI services.
- Excessive permissions granted to AI agents, increasing the impact of misuse or compromise.
- Third-party AI dependencies, where AusNet relies on vendor-provided AI functionality with limited visibility of security controls, data handling and operational dependencies.
- Inadequate resilience and recovery arrangements for business and operational processes that depend on AI-enabled technologies.

Vulnerabilities created or found by internal or external AI must be addressed in a timely manner. Refer to the section on recent events below for specific examples related to inappropriate governance and controls when adopting AI tools.

AI defence to augment AESCSF Version 2

The Australian Energy Sector Cyber Security Framework (AESCSF) Version 2 released in October 2023 provides a comprehensive maturity framework for managing cyber security risks across the energy sector and was updated to address technologies and the threat landscape at that time.

However, AESCSF Version 2 predates the recent acceleration in frontier and agentic AI capabilities and does not define control requirements to protect from AI risks and threats and the potential cascading failures across interconnected AI-enabled systems. These risks are addressed more directly in ACSC publications and Protective Security Policy Framework (PSPF)[5] guidance, including the emerging concept of a "vulnerability storm." This guidance demonstrates that frontier and agentic AI constitute a rapidly evolving risk domain that extends beyond the specific practices and maturity requirements currently defined within AESCSF Version 2. As a result, AI-related cyber risk should be treated as an emerging strategic risk domain that requires management in addition to AESCSF compliance.

New technology providing opportunities

The ACSC, together with cyber security agencies from Canada, New Zealand and the United Kingdom, highlight that AI is rapidly changing the cyber threat landscape.[6] As malicious actors increasingly use AI to improve the speed, scale and sophistication of cyber attacks, organisations must evolve their cyber security practices to keep pace. The guidance emphasises that organisations relying heavily on manual cyber security processes may struggle to effectively identify, prioritise and respond to growing cyber risks.

The guidance positions AI as a powerful enabler of cyber defence rather than a replacement for existing security controls. AI can be applied across the full cyber security lifecycle, including governance, asset and risk identification, protection, threat detection, incident response and recovery. When adopted responsibly, AI can improve decision-making, automate repetitive activities, accelerate investigations and help security teams focus on higher-value risk management activities.

These agencies detail a number of key opportunities for organisations:

- Improve risk prioritisation by using AI to analyse large volumes of security data and identify the most critical threats and vulnerabilities that can be "chained" together.
- Enhance threat detection through faster identification and analysis of suspicious activities, emerging threats and security events.
- Accelerate incident response and recovery by supporting investigation, decision-making and remediation activities.
- Reduce manual effort by automating repetitive cyber security tasks, allowing scarce cyber specialists to focus on higher-value activities.

[5] the Australian Government's framework for protecting people, information and resources through policies covering governance, risk, information security, technology, personnel security and physical security. The relevant document is PSPF Policy Advisory 001-2026 – Cyber Security Readiness in the Frontier AI Era

[6] https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/opportunities-for-ai-in-cyber-defence

- Strengthen cyber resilience by applying AI across governance, protection, detection, response and recovery functions while maintaining robust security controls and oversight.

A key message is that strong cyber security fundamentals remain essential. Human oversight, governance, Secure by Design principles, identity and access management, patching, monitoring and incident response capabilities must remain in place. Poorly governed AI systems can introduce new attack paths and risks, meaning organisations should adopt AI in a controlled and secure manner.

Additionally, AI should therefore be viewed as a force multiplier for cyber defence rather than a replacement for existing controls. When applied appropriately, it can enhance threat detection, accelerate investigation and response activities, and automate repetitive cyber security tasks, enabling security teams to manage a higher volume of threats with greater speed and effectiveness while maintaining appropriate oversight and governance.

Examples of recent events

The ASD has stated that the cyber threat to Australian businesses has accelerated due to the advancement of AI. ASD responded to more than 1,200 cyber security incidents in FY2024-25, an 11% increase from the previous year and notified Australian organisations of potentially malicious cyber activity more than 1,700 times, an 83% increase from the previous year.

ASD guidance says:

> *"Over the past two years, AI capabilities have advanced rapidly, with OpenAI warning as early as December 2025 that forthcoming frontier models will pose a high cyber security risk. It is important to remember that there are also opportunities for the cyber security industry to use these frontier models to mitigate cyber threats before they occur, a sentiment shared by the National Cyber Security Centre – United Kingdom"*[7]

The following summaries describe five different events where AI identified material risks or demonstrated new and advanced capabilities of AI that could be used to exploit systems. They demonstrate autonomous cyber attack capability, zero day risk, risk to critical infrastructure and operational technology and strategic risk and governance implications.

- **Claude Mythos 32-Step Corporate Network Attack Simulation (2026):** During testing by the UK AI Security Institute, Claude Mythos became the first AI model reported to autonomously complete a simulated 32-step corporate network intrusion involving reconnaissance, privilege escalation, lateral movement and full network compromise. The exercise demonstrated that frontier AI models can automate many tasks previously requiring skilled penetration testers or threat actors, increasing the speed and scale of sophisticated cyber attacks.
- **Firefox Vulnerability Discovery using Claude Mythos (2026):** Mozilla used Claude Mythos Preview to analyse the Firefox code base, identifying 271 vulnerabilities that were subsequently fixed. The case highlighted how AI can dramatically accelerate vulnerability discovery, reducing the time available for organisations to identify and patch weaknesses before adversaries can exploit them
- **Project Glasswing (2026):** Following successful testing of Claude Mythos, Anthropic launched Project Glasswing, a collaboration involving major technology companies to identify and remediate vulnerabilities in critical software. The initiative demonstrated that frontier AI can uncover software vulnerabilities at a scale and speed previously unattainable through conventional security testing, creating both defensive opportunities and increased cyber risk if similar capabilities become widely available to attackers
- **Agentic AI Security Risks in Critical Infrastructure (2026):** Joint guidance from the ACSC, CISA and NSA highlighted emerging risks associated with autonomous agentic AI systems operating in critical infrastructure environments. Identified risks included excessive privileges, expanded attack surfaces, behavioural misalignment and reduced accountability. The case demonstrated that poorly governed AI agents could create new pathways for compromise of enterprise and operational technology systems.
- **The Emerging "Vulnerability Storm" Risk (2026):** Australian Government cyber security guidance warned of a potential "vulnerability storm", where frontier AI models can discover vulnerabilities faster than organisations can remediate them. The risk is particularly significant for operators of critical infrastructure and legacy systems because AI may substantially shorten the time between vulnerability discovery and exploitation, increasing exposure to zero-day and previously undiscovered weaknesses.

[7] Frontier models and their impact on cyber security | Cyber.gov.au

Additionally, there have been numerous examples where AI adoption without appropriate governance and controls has adversely impacted organisations and their customers. In the three cases detailed below, the underlying issue was not the AI technology itself, but insufficient governance over how AI was used, monitored, controlled or contained, allowing operational, legal, security and reputational risks to materialise and impact the customers who rely on their services.

- **Hugging Face Incident (2026).** During a controlled cyber security evaluation, advanced AI agents escaped their intended testing environment, gained internet access and autonomously compromised parts of Hugging Face's infrastructure while attempting to achieve their assigned objective. The incident highlighted how insufficient containment, monitoring and governance of highly capable AI systems can result in unintended and potentially harmful actions beyond their authorised scope.
- **Air Canada Chatbot (2024).** Air Canada was found liable after a customer relied on incorrect information provided by the airline's chatbot regarding bereavement fares, resulting in financial loss to the customer. The case demonstrated that organisations remain accountable for AI-generated advice and that inadequate oversight of customer-facing AI can create legal, financial and reputational risks.
- **Samsung ChatGPT Data Leak (2023).** Samsung employees uploaded confidential source code, engineering data and internal meeting information into ChatGPT to assist with work tasks, inadvertently exposing sensitive intellectual property to an external AI platform. The incident highlighted the risks of deploying AI without clear policies, data governance controls and staff awareness regarding what information can be shared with AI tools.

The following two examples are related to cyber attacks directed at utilities or common utility assets:

- **The FortiBleed campaign (2026).** The FortiBleed campaign revealed how cybercrime is becoming increasingly automated and AI-enabled, with attackers using large-scale scanning, credential harvesting and password-spraying techniques to compromise more than 21,000 organisations across multiple technologies, including Fortinet, Sophos, Synology and Microsoft SQL Server systems. Investigators identified the operation as an Initial Access Broker campaign that used AI-assisted tools to accelerate malware development, automate attack workflows and scale intrusions, demonstrating how poor cyber hygiene and exposed internet-facing systems can now be exploited at unprecedented speed and scale.
- **Water utility OT infrastructure (2026)**. Attackers used commercial AI models to undertake a cyber intrusion against a Mexican municipal water utility. They used Anthropic's Claude and OpenAI GPT to accelerate reconnaissance, environment mapping, tool development and intrusion planning, ultimately attempting to move from the organisation's IT network toward its operational technology (OT) environment. While the attackers did not successfully breach the industrial control systems, the incident demonstrated that AI can significantly reduce the effort required to identify critical infrastructure assets, develop attack pathways and automate offensive cyber activities, highlighting the growing need for strong IT/OT segmentation, monitoring and foundational cyber security controls in critical infrastructure environments.

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2. Needs identification

The purpose of this section is to detail the drivers of expenditure on AI Defence capabilities for the TRR 2027-32 regulatory period. This investment is focused on developing and uplifting our AI-enabled cyber security defences in line with the increasing threat landscape and industry guidance.

The key drivers for this program are:

- Compliance with clause 8A of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023 (**CIRMP Rules**) as amended.
- Following guidance from DoHA, ASD and AEMO that critical infrastructure businesses should address AI threats
- Closing gaps in our IT and OT systems that create vulnerabilities to the new capabilities of AI being adopted
- Ensuring AusNet's risk profile remains acceptable.

These key drivers are described in the sections below.

2.1. Regulatory and compliance obligations

CIRMP Amendment Rules

The CIRMP Amendment Rules introduced specific requirements for critical infrastructure entities to identify, assess and manage risks arising from emerging technologies, including AI. The CIRMP Amendment Rules do not prescribe detailed AI policies or acceptable-use rules. Instead, they require AusNet to:

- Assess and document risks from AI and other emerging technologies.
- Implement governance processes to control AI deployment.
- Consider AI as an emerging cyber threat vector.
- Implement cyber security controls capable of defending against AI-enhanced attacks.
- Maintain ongoing governance, monitoring and assurance of AI-related risks.

The most relevant rules included in the CRIMP Rules as amended are shown in **Table 2**. The requirement is that AusNet must establish and maintain a process in the CIRMP to minimise or eliminate risks caused by the use of emerging technologies (ie AI) by AusNet, or caused by the use of emerging technologies by malicious actors.

This sets a clear obligation on AusNet to invest in governance of AI use and defence against AI threats.

Table 2 – Summary of most relevant CIRMP Rules requirements (as amended)

Clause	Relevance to AI
8A(2)(c)	As far as is reasonably practicable, to ensure controls are in place to minimise or eliminate risks of an organisation's own use or deployment of AI and other emerging technologies[8].
8A(2)(d)	As far as is reasonably practicable, to ensure controls are in place to minimise or eliminate risks arising from AI and other emerging technologies being used against the organisation.
8A(5)	Requires appropriate measures (governance) to ensure controls are in place to minimise or eliminate risks to the critical infrastructure assets.

[8] The Explanatory Statement published with the CIRMP Amendment Rules clarifies that the term "advanced, novel or emerging technology" is intended to be broad and expansive to avoid limiting its scope and to capture technology that responsible entities may already be aware of and implementing (such as AI) and technology that is not yet available (such as quantum cryptography).

General cyber security obligations

Authorities such as AEMO, ASD and ACSC are increasingly taking AI into account with respect to cyber security requirements. However, due to the pace of AI development, frameworks such as AESCSF do not necessarily remain current and suitably address the latest threats. In general, the suite of cyber security requirements and obligations that AusNet is subject to require AusNet to consider the risk to the safe and secure operation of the electricity network that are created by AI technologies. **Table 3** identifies key regulatory obligations that are critical to AusNet's cyber security practices.

Table 3 – Regulatory obligations underpinning cyber security functions

Regulatory Obligation	Description of obligations
Security of Critical Infrastructure Act 2018 (Cth)(SOCI Act), including 2024 amendments	The SOCI Act seeks to manage national security risks in Australia's critical infrastructure including energy. The obligations include: • a requirement to register Critical Infrastructure Assets • mandatory cyber incident reporting to the Australian Cyber Security Centre Further amendments made in 2024 added obligations in relation to protecting business critical data, obligations to address deficiencies in CIRMPs if requested, and further details in relation to the definition and appropriate handling and disclosure of protected information.
Privacy Act 1988 (Cth)	The obligations require us to maintain strong controls and security on the accessibility of customer data as well as appropriate availability of data.
National Electricity Law, as included in a schedule to the *National Electricity (South Australia) Act 1996* (SA), and subordinate legislation (eg National Electricity Rules, **NER**)	Under clause 4.11.2(c) of the NER, AusNet must comply with AEMO's Standard for Power System Data Communications which operates in parallel to the SOCI Act identified above. Chapter 4 of the NER requires that cyber, physical and network security considerations are appropriately addressed by all parties including through robust programs and reporting frameworks to adequately and continuously manage security risks that could adversely impact power system communications and supporting systems and infrastructure.
Cyber Security Act 2024 (Cth)	Imposes a requirement for reporting of certain cyber attacks and ransom payments.

Engagement with authorities

AusNet has undertaken significant engagement with relevant [SOCI ACT PROTECTED].

There is a clear consensus across these entities that AI is an emerging risk that need to be addressed. Although there have not been any direct mandates specific to AI risks, or how they should be addressed, clause 8A of the CIRMP Rules provides an obligation to address the risk of emerging technologies. Recognising these risks, ASD has released several publications providing guidance on the secure adoption and use of AI technologies. [9] [10] [11]

2.2. Current state of maturity

[SOCI ACT PROTECTED]

[9] Opportunities for AI in cyber defence | Cyber.gov.au
[10] Careful adoption of agentic AI services | Cyber.gov.au
[11] Frontier models and their impact on cyber security | Cyber.gov.au

[SOCI ACT PROTECTED]

2.3. Risk assessment

[SOCI ACT PROTECTED]

Artificial intelligence is changing the cyber threat landscape by increasing attacker capability, accelerating the identification of weaknesses and lowering barriers to entry for malicious actors. As a result, the likelihood and potential impact of cyber incidents is increasing across the critical infrastructure sector.

The inherent risk considers the related programs (refer to Section 0) that AusNet is planning to implement during the next regulatory period: the cyber security program to achieve AESCSF V2 SP3; CI Fortify to enable separation of IT and OT systems; and Patching to reduce the exposure of vulnerabilities across IT and OT environment. These programs do not specifically address the risks arising from the increasing use of AI by AusNet, its vendors and third parties, or the growing use of AI by cyber threat actors. As set out in Section 1, these risks are increasing rapidly.

[SOCI ACT PROTECTED]

Consequence methodology

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Outcome

Our risk assessment shown in Error! Reference source not found.**1** demonstrates the risk to AusNet from the increase in t hreat environment if these risks are not mitigated.

[SOCI ACT PROTECTED]

2.4. Whole of AusNet implementation and transmission network cost allocation

Due to the integrated nature of our digital systems across our electricity transmission, electricity distribution and gas distribution networks, the CIRMP Amendment Rules and expectations for timely patching and management of risks from emerging technologies (i.e., AI) affect all of AusNet's services.

While the consequences and risks being managed vary across our three networks, the required mitigation actions are a common requirement. It is not possible to implement different approaches to cyber security, including AI governance and AI-enabled cyber defence, across our networks as a consistent level of maturity is required to prevent "weakest-link" exposures.

AusNet's approach to meet the requirements of the CIRMP Amendment Rules 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 initiatives for a specific network have been 100% allocated to that network, while

investments that are shared across networks (such AI defence capabilities) 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.

3. Options Assessment

In developing our AI for Cyber Defence business case we have identified potential options in consultation with relevant authorities (DoHA, ASD, AEMO) and leading AI businesses and providers. We have assessed the options against the identified needs including the new regulatory obligations created by the CIRMP Amendment Rules, the identified gaps in our current capabilities, and the resulting risk to our business, and ultimately provision of electricity services to our customers.

As stated in Section 0, our needs have been identified on the basis that our cyber security program is fully implemented with achievement of AESCSF V2 SP3. We note that the need for investment in defence against new and emerging technologies (termed AI Defence) is a new requirement and is not covered by AESCSF V2 SP3 nor our cyber security program or other investments being planned in response to the CIRMP Amendment Rules.

We have taken a staged approach to options assessment where we identified whether options were credible or non-credible then undertook detailed analysis on the credible options. Where options were found to be non-credible, we have only provided our reasoning for why they were non credible. Cost estimates have been developed using non-binding indicative vendor pricing, and input from internal SMEs.

We have also considered the suite of cyber security related projects that are planned to address AESCSF V2 SP3 (as submitted as part of our initial TRR proposal) and the new projects focused on addressing the requirements of the CIRMP Amendment Rules to ensure there are no overlaps in scope. Further information demonstrating there is no overlap between the projects is provided in Section 0.

3.1. Non-credible options

Our options analysis found that a 'do nothing' option where our current level of maturity with respect to AI defence for cyber security would be maintained is not a credible option as:

- This would not enable compliance with the CIRMP Rules rule 8A
- The threat landscape is evolving rapidly and maintaining current maturity (existing systems and practices) is not aligned with best industry practice and will expose AusNet and its customers to unacceptable risk. This will effectively result in our risk exposure increasing as AI technologies advance and new technologies emerge.

Therefore, this option has not been considered further and serves as the base case for assessing the remaining options.

3.2. Assessment of credible options

Our analysis identified three credible options:

[SOCI ACT PROTECTED]

As required by the AER's guidelines, and consistent with the CIRMP Amended Rules expectations, AusNet assessed this range of credible options considering risk reduction benefits, implementation costs and net present value.

[SOCI ACT PROTECTED]

This options assessment is discussed in the following sections. Detailed scope for the initiatives proposed in these options is provided in **Appendix A**.

3.2.1. Option 1 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Advantages

- This is the least cost option that will provide the minimum foundation for control and management of AI capabilities.

[SOCI ACT PROTECTED]

Our analysis found that this option is unlikely to address the full obligations under the CIRMP Rules rule 8A(2)(d) and that the risk reduction achieved by further scope options is justified by higher net present value. Therefore we do not recommend this option.

3.2.2. Option 2 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Advantages

- Addresses all identified gaps so it reduces risk to an acceptable level.

[SOCI ACT PROTECTED]

Disadvantages

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Table 12 – Summary option 2 costs ($'million, FY25, transmission network allocation)

Cost item	RY2028	RY2029	RY2030	RY2031	RY2032	Total
Capex	[SOCI ACT PROTECTED]					
Opex						
Total						

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.2.3. Option 3 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Advantages

- Addresses all identified gaps so it reduces risk to an acceptable level.

[SOCI ACT PROTECTED]

Disadvantages

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Cost estimate for Option 3 is shown in Table 13.

Table 13 Summary of option 3 costs ($'million, FY25, transmission network cost allocation)

Cost item	RY2028	RY2029	RY2030	RY2031	RY2032	Total
Capex	[SOCI ACT PROTECTED]					
Opex						
Total						

[SOCI ACT PROTECTED]

4. Recommended option

Our analysis identified the need for investment to meet the requirements of the CIRMP Rules clause 8A in relation to emerging technologies, to address gaps identified in our AI defence capabilities that are beyond the scope of AESCSF V2 SP3. Our analysis identified four options of which one was deemed non-credible and one did not fully address the requirements of the CIRMP Rules rule 8A(2)(d). Two fully addressed the need.

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Appendix A – Detailed scopes of work

Table 16 provides detail on each of the proposed initiatives investments under the AI for Cyber Defence business case and their respective costs.

Table 16 – Initiatives planned to be implemented for preferred Option 2

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[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

ausnet.com.au