AusNet

Transmission Revenue Reset

TRR (2027-32)

Patching Business Case

Tuesday, 1 September 2026

Table of contents

Document history

DATE	VERSION	COMMENT
7/08/2026	V1.0	Initial draft business case for review
26/08/2026	V2.0	Revised business case incorporating input
31/08/2026	V3.0	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
4.2.10 AusNet - IBM - Patching Cost Basis Report - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	IBM
4.2.17 AusNet - GE - Patching Cost Basis Report - 1 Sep 2026 - SOCI ACT PROTECTED	V1.0	GE Vernova

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

AusNet relies on a large and growing portfolio of digital systems to operate and maintain our transmission network, supporting critical operational functions and delivering electricity services to customers. As these systems become increasingly interconnected and software-dependent, maintaining them in a secure and supported state becomes a critical component of managing cyber risk. Recent guidance from government agencies and industry stakeholders highlights that advances in artificial intelligence (AI) are accelerating the discovery and exploitation of software vulnerabilities, reducing the time available for organisations to identify, assess and remediate security weaknesses. This trend is particularly significant for operators of critical infrastructure such as electricity networks.

The need to invest

[SOCI ACT PROTECTED]

Options assessment

Based on understanding of current risks and capabilities, AusNet identified and evaluated three credible investment options to enhance our patching capabilities. These are described in **Table 1** with their associated cost and assessment of residual risk once implemented.

Table 1 – Patching investment options evaluated

#	OPTION ASSESSMENT	CAPEX ($M)	OPEX ($M)	NPV ($M)
1	Option 1 [SOCI ACT PROTECTED]			
2	Option 2 [SOCI ACT PROTECTED].	[SOCI ACT PROTECTED]		
3	Option 3 [SOCI ACT PROTECTED]			

AusNet recommends **Option 2**, which delivers the highest NPV and provides the most balanced outcome across risk reduction, compliance and cost efficiency.

[SOCI ACT PROTECTED]

The assessment found that this option addresses the requirements of the CIRMP

Amendment Rules, reduces residual cyber risk to within AusNet's risk appetite and provides the highest overall value of the options considered.

[SOCI ACT PROTECTED]

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 potential for severe consequences. 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 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 and the capabilities of the new frontier AI models has been repeatedly demonstrated this year to be able to find existing but previously unknown vulnerabilities and then quickly exploit these to attack systems. This includes complex attacks that chain multiple system attributes together to access deep into the organisations core internal systems.

This has highlighted the need to both keep systems up to date with the latest patches available to address identified vulnerabilities and implement improved – more frequent and rigorous – testing practices to identify and fix vulnerabilities before they can be exploited.

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, can be updated to address this risk. 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.

Growing 'Zero-day' risks

A major consequence of frontier AI is the increased risk associated with 'zero-day' and previously undiscovered vulnerabilities.

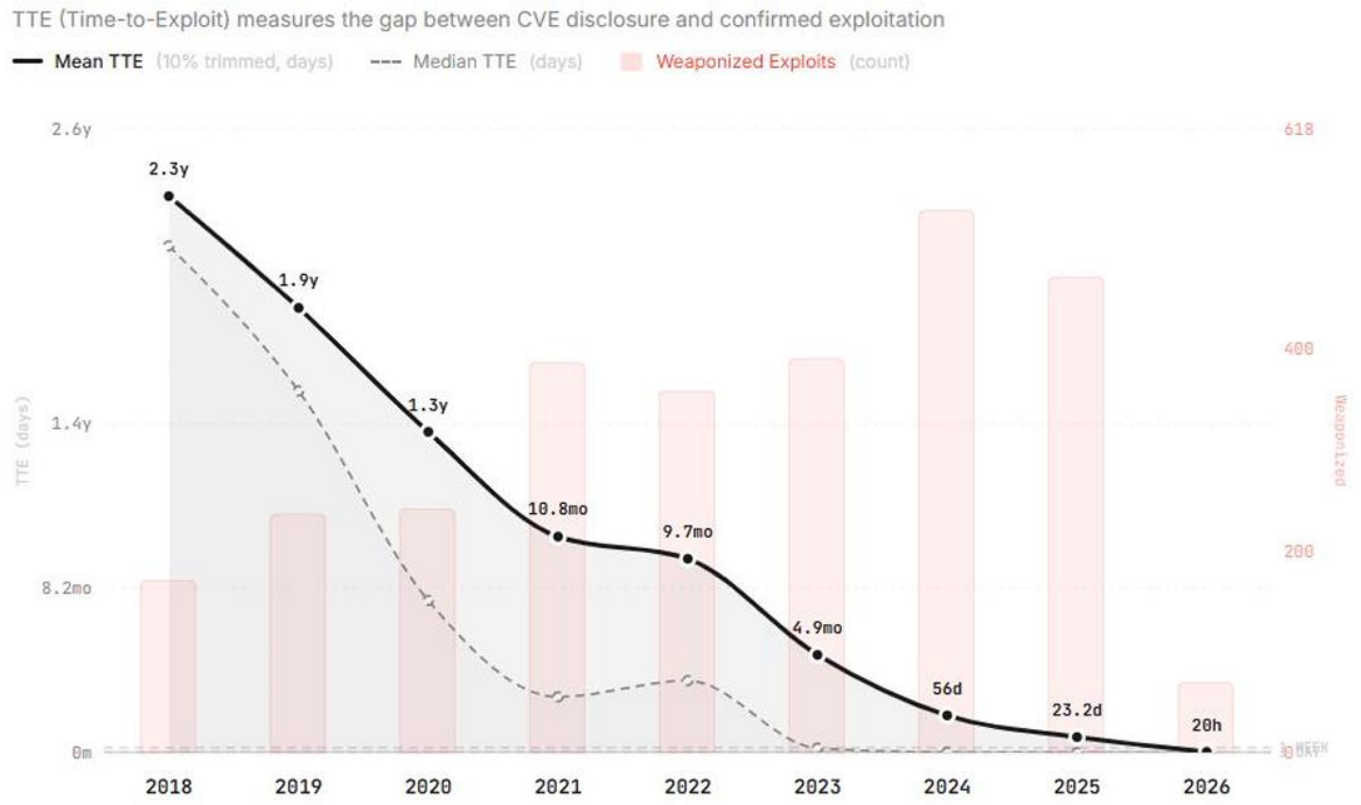
AI-related zero-day risk is the risk that a previously unknown vulnerability, attack technique or AI-enabled threat emerges before effective controls, detection mechanisms or patches are available, resulting in increased cyber exposure and reduced response time (i.e., measured in hours or days) before the AI can create an attack to exploit the vulnerability.

ACSC guidance highlights that frontier AI models can identify vulnerabilities that have remained hidden despite extensive human review and automated testing. An assessment of the time taken historically to move from identifying

[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

a vulnerability to creating an attack has been reducing during the past eight years, as shown in **Figure 1**. As AI capabilities improve, the time between vulnerability discovery and exploitation is expected to continue to shrink.

Figure 1 From Vulnerability to Exploitation



Source: *The "AI Vulnerability Storm": Building a "Mythos-ready" Security Program*

The Protective Security Policy Framework (PSPF)[5] Policy Advisory describes this as a potential "vulnerability storm", where AI accelerates the identification and exploitation of weaknesses faster than organisations can patch and remediate them. Legacy systems, technical debt, weak cyber hygiene and delayed patching become increasingly significant risk factors in this environment.

Patching to augment AESCSF Version 2

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

However, frontier AI and agentic AI represent a rapidly evolving area that extends beyond the specific practices and maturity requirements currently defined within AESCSF Version 2. The pace of AI capability development, AI-enabled vulnerability discovery, agentic AI risks, and the emerging concept of a "vulnerability storm" are addressed in recent ACSC and Protective Security Policy Framework (PSPF)[5] guidance rather than through explicit AESCSF V2 practices.

As a result, AI-related cyber risk should be viewed as an emerging strategic risk domain that complements, rather than replaces, AESCSF compliance.

A focus on patching reduces the number of vulnerabilities and therefore the attack surface that can be targeted by bad actors and these new frontier AI models. To achieve that, firstly the vulnerabilities need to be known, a capability provided by scanning tools or via vendor communications. These vulnerabilities need to be prioritised for remediation, through a system supporting the tracking of the vulnerability, the prioritisation, and the availability of patches. Unless the patch is deployed into production the risk remains. The rapid application of the patch is supported by automated testing and rapid deployment through managed environments.

[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

New technology is providing opportunities

While AI increases cyber risk, it is still dependant on available, unpatched vulnerabilities and the ability to chain these together into a successful breach. Key to mitigating this is reducing the number of available vulnerabilities, with a focus on the right, high risk, vulnerabilities and rapid implementation of the mitigation. Patching represents the primary mitigation and is addressed in this business case. This aligns with several opportunities identified by ACSC including:

- Strengthen prioritisation of cyber risks
- Improve detection and/or awareness of threats and vulnerabilities
- Support faster response and recovery
- Reduce reliance on repetitive manual tasks.
- Identification and remediation of software vulnerabilities before attackers can exploit them

These form part of strong cyber security fundamentals. Human oversight, governance, identity and access management, network segmentation, monitoring, patch management and incident response remain essential. AI is both a cause of the increasing cyber risks and an opportunity to improve cyber defences. AI defence is considered an addition, on top of this foundation, which has been address separately in the AI Defence business case.

Examples of recent events

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"* [6]

The following five 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 Australian Cyber Security Centre (ACSC), the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) highlighted emerging risks associated with autonomous agentic AI systems operating in critical infrastructure environments. Identified risks included excessive privileges, expanded attack surfaces,

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

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.

The "Firefox Vulnerability Discovery using Claude Mythos (2026)" described above demonstrates how the adoption of AI frontier models by vendors within their own ecosystem will result in vendors identifying increasing number of vulnerabilities in their own products. This increases the number of vulnerability notification and patches AusNet will expect to receive from all of our product vendors. This will add extra load on AusNet's patching processes.

The "vulnerability storm" state above also highlights expectation that frontier AI models can discover vulnerabilities faster than organisations can remediate them. Having an optimised and efficient patching process will mitigate some of this by ensuring the majority, if not all, of the high-risk vulnerabilities are patched as rapidly as practicable.

The risks have resulted in cyber attacks directed at utilities or common utility assets, as the below example describes:

- **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. This examples specifically relates to this patching business case in that active and rapid patching would have reduce the vulnerabilities identified in the reconnaissance phase of the attack.

Relationship to other programs

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2. Needs identification

The purpose of this section is to detail the drivers of non-recurrent expenditure on vulnerability identification, assessment and patching capabilities for the TRR 2027-32 regulatory period. This investment is focused on developing and uplifting our patching capabilities in line with the increasing threat landscape and industry guidance.

The key drivers for this program are:

- Compliance with clause 8A of the CIRMP Rules as amended
- Acting on guidance from AEMO, ASD and DoHA that critical infrastructure businesses should address new and emerging technology threats, such as use of AI tool by malicious actors, which shorten time from identification to exploitation, thus increasing the importance of rapid patching
- 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 define patching as a risk mitigation. The Rules require AusNet, as a critical infrastructure owner, to minimise or eliminate any material risk of breach due to unpatched vulnerabilities and mitigate the relevant impact on the critical infrastructure, so far as is reasonably practicable to do so.

The CIRMP Amendment Rules do not prescribe detailed requirements for maintaining systems and software with updates and/or patches. The requirement is to '…so far as is reasonably practicable, … minimise or eliminate…' the risks caused by the vulnerabilities.

In the context of cyber security, we interpret 'so far as is reasonably practicable' to mean that AusNet must take all feasible and sensible steps while balancing the level of risk against the time, difficulty to implement, and cost of the solution. It does not require risk to be eliminated completely but action must be taken up to a point where the cost, complexity or feasibility of the solution is grossly disproportionate to the level of risk reduction achieved.

The most relevant clauses from the CRIMP Rules as amended are shown in **Table 4**, including additional context provided by the Explanatory Statement to the CIRMP Amendment Rules. They impose a clear obligation on AusNet to invest to improve the testing and assessment of system vulnerabilities, and development and/or deployment of patches to mitigate or eliminate the risk of those vulnerabilities.

Table 4 – Summary of most relevant CIRMP Rules requirements

Rule	Relevance to patching
8A(2)(a)	So far as it is reasonably practicable to do so, minimise or eliminate material risks arising from failure to patch or update operating or security systems in a timely manner.
8A(2)(b)	So far as it is reasonably practicable to do so, mitigate risks caused by legacy equipment through replacement or other controls. Unsupported and end-of-life technologies often have vulnerabilities which are not addressed by vendor patches or that may not have been previously identified.
8A(2)(c)-(d)	Use of new technologies to rapidly scan the systems and software for vulnerabilities to enable identification, assessment and prioritisation of vulnerabilities in order to develop and deploy patches and reduce attack paths and surfaces. *NOTE: Both this Patching program and the AI Defence program provide a functionality of scanning code and systems, respectively, to identify vulnerabilities. The scope for the two programs are unique and complimentary, they do not overlap. Refer to Section 1 for more details.*

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 with the latest threats. In general, the suite of cyber security requirements and obligations placed upon AusNet require AusNet to consider risks to the safe and secure operation of the electricity network that are created by AI technologies. **Table 5** identifies key regulatory obligations that are critical to AusNet's cyber security practices.

Table 5 – 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 authorities including DoHA, ASD and AEMO in relation to cyber security in the lead up to, and since the release of, the CIRMP Amendment Rules.

Guidance from these authorities is that AI is an emerging risk that needs to be addressed. Although there have not been any direct mandates specific to AI or how it should be addressed, requirements of rule 8A of the CIRMP Amendment Rules provides obligations to address emerging technologies. Rule 8A(2)(a) makes specific reference an obligation to eliminate the risk of failure to patch in a timely manner.

AusNet have actively reviewed our Revised Proposal programs with these relevant authorities to confirm alignment and will continue to maintain this engagement through the 2027-32 regulatory period.

2.2. Current state of maturity

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2.3. AusNet's approach for timely patching

The CRIMP Amended Rules rule 8A rules require timely patching without defining the specific target or targets. As detailed in the prior Section, AusNet's current systems and practices limit our patching speed and cycle time.

[SOCI ACT PROTECTED]

2.4. Risk assessment

This section provides an assessment of the base case risk if no action is taken to address the requirements of CIRMP Rules rule 8A, and the increasing threat from inadequate patching practices in the context of AI and other emerging technologies.

[SOCI ACT PROTECTED]

Methodology for assessing potential consequences

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

Methodology for assessing likelihood

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

2.5. 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 timely patching and emerging technology risk management, 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 are 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 as patching tooling and AI defence) 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 development of our TRR Revised Proposal, and consistent with the CIRMP Amendment Rules expectations, we have evaluated a range of options to address the identified gaps and risks resulting from our current patching systems and processes.

As stated in Sections 1 and 2, our program needs have been identified, and options evaluated, on the basis that our cyber security program is fully implemented and we achieve AESCSF V2 SP3. [SOCI ACT PROTECTED]

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 provided our reasoning as to this assessment.

3.1. Non-credible options

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

- This would not enable compliance with the Enhanced CIRMP Rules Clause 8A
- The threat landscape is evolving 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 exiting 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

[SOCI ACT PROTECTED]

3.2.1. Option 1 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.2.2. Option 2 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

3.2.3. Option 3 – [SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

[SOCI ACT PROTECTED]

4. Recommended option

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

[SOCI ACT PROTECTED]

Appendix A – Detailed scope of work

[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