EMCa

energy market consulting associates

AusNet 2026 - 2031 Regulatory Proposal

REVIEW OF PROPOSED EXPENDITURE ON CYBER SECURITY

[redacted]

Report prepared for:

AUSTRALIAN ENERGY REGULATOR (AER)

August 2025

Preface

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be allowed for the prescribed distribution services of AusNet from 1st July 2026 to 30th June 2031. The AER's determination is conducted in accordance with its responsibilities under the National Electricity Rules (NER).

This report covers a particular and limited scope as defined by the AER and should not be read as a comprehensive assessment of proposed expenditure that has been conducted making use of all available assessment methods nor all available inputs to the regulatory determination process. This report relies on information provided to EMCa by AusNet. EMCa disclaims liability for any errors or omissions, for the validity of information provided to EMCa by other parties, for the use of any information in this report by any party other than the AER and for the use of this report for any purpose other than the intended purpose. In particular, this report is not intended to be used to support business cases or business investment decisions nor is this report intended to be read as an interpretation of the application of the NER or other legal instruments.

EMCa's opinions in this report include considerations of materiality to the requirements of the AER and opinions stated or inferred in this report should be read in relation to this over-arching purpose.

Except where specifically noted, this report was prepared based on information provided to us prior to 30 May 2025 and any information provided subsequent to this time may not have been taken into account. Some numbers in this report may differ from those shown in AusNet's regulatory submission or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell

Managing Director
psell@emca.com.au

Prepared by

Mark de Laeter, Paul Sell and Eddie Syadan

Date saved

26/09/2025 10:21 AM

Version

Final v2

Energy Market Consulting associates

ABN 75 102 418 020

Sydney Office

L25, 100 Mount Street, North Sydney NSW 2060
PO Box 592, North Sydney NSW 2059
+(61) 2 8923 2599
contact@emca.com.au
www.emca.com.au

Perth Office

L28, 140 St Georges Terrace, Perth WA 6000
contact@emca.com.au
www.emca.com.au

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

Term	Definition
ACSC	Australian Cyber Security Centre
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
AI	Artificial Intelligence
ASD	Australian Signals Directorate
C2M2	Cyber Security Maturity Model
CAPEX	Capital expenditure
CIRMP	Critical Infrastructure Risk Management Program
CONF	Confidential
Current RCP	2022-2026 RCP
DNSP	Distribution Network Service Provider
E-CAT	Electricity Criticality Assessment Tool
ECSO	Enhanced Cyber Security Obligations
EDPR	Electricity Distribution Price Review
EEMM	Essential Eight Maturity Model
ICT	Information and Communication Technology
IR	Information Request
IT	Information Technology
MIL-1	Meeting Maturity Indicator Level One
NER	National Electricity Rules
Next RCP	2027-2031 RCP
NPV	Net Present Value
NSP	Network Service Provider's
Opex	Operational expenditure
OT	Operational Technology
RCP	Regulatory Control Period
RP	Regulatory Proposal
SOC	Security Operations Centre
[redacted]	[redacted]
[redacted]	[redacted]

Term	Definition
SP	Security Profile under the AESCSF
TOTEX	Total expenditure

1 INTRODUCTION

The AER has asked us to review and provide advice on aspects of Ausnet's proposed expenditures over the 2026-31 Regulatory Control Period (next RCP) relating to information and communication technology (ICT), consumer energy resources (CER) related ICT and cyber security.

For reasons of confidentiality, this report on our assessment of AusNet's cyber security program is separate from our other reports for the AER pertaining to AusNet's forecast expenditure for ICT and CER.

Our review is based on information that Ausnet provided and on aspects of the NER relevant to assessment of expenditure allowances.

1.1 Purpose of this report

1. The purpose of this report is to provide the AER with a technical review of aspects of the expenditure that Ausnet has proposed in its regulatory proposal (RP) for next RCP'

2. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed expenditures allowance as an input to its Draft Determination on Ausnet's revenue requirements for the next RCP.

1.2 Scope of requested work

3. Our scope of work, covered by this report, is as defined by the AER. Relevant aspects of this are as summarised in Figure 1.1.

Figure 1.1: Scope of work covered by this report

Scope of work covered by this report.

The scope of this review, as requested by the AER, covers the following.

- Capex (ex ante)
  - Cyber security
- Opex step changes related to:
  - Cyber security

4. Other aspect of Ausnet's expenditures, including repex, augex and opex (pole inspection and hazard tree reduction), CER and other ICT related expenditures are covered in our 'technical' and 'ICT' reports.

1.3 Our review approach

5. In conducting this review, we first reviewed the RP documents that Ausnet has submitted to the AER. This includes a range of appendices and attachments to Ausnet's RP and certain Excel models which are relevant to our scope.

6. We next collated several information requests. The AER combined these with information request topics from its own review and sent these to Ausnet.

7. In conjunction with AER staff, our review team met with Ausnet at its offices on 2 – 4 April 2025. Ausnet presented to our team on the scoped topics, and we had the opportunity to engage with Ausnet to consolidate our understanding of its proposal.

8. Ausnet provided the AER with responses to information requests and, where they added relevant information, these responses are referenced within this review.

9. We have subjected the findings presented in this report to our peer review and Quality Assurance processes and we presented summaries of our findings to the AER prior to finalising this report.

1.3.1 Conformance with NER requirements

10. In undertaking our review, we have been cognisant of the relevant aspects of the NER under which the AER is required to make its determination and relevant AER Guidelines.

Capex objectives and criteria

11. The most relevant aspects of the NER in this regard are the 'capital expenditure criteria' and the 'capital expenditure objectives.' Specifically, the AER must accept the Network Service Provider's (NSP) capex proposal if it is satisfied that the capex proposal reasonably reflects the capital expenditure criteria, and these in turn reference the capital expenditure objectives.

12. The NER's capital expenditure criteria and capital expenditure objectives are reproduced in Figure 1.2 and Figure 1.3.

Figure 1.2: NER capital expenditure criteria

> **NER capital expenditure criteria**
>
> The *AER* must:
>
> *(1) subject to subparagraph (c)(2), accept the forecast of required capital expenditure of a Distribution Network Service Provider that is included in a building block proposal if the AER is satisfied that the total of the forecast capital expenditure for the regulatory control period reasonably reflects each of the following (**the capital expenditure criteria**):*
>
> *(i) the efficient costs of achieving the capital expenditure objectives;*
>
> *(ii) the costs that a prudent operator would require to achieve the capital expenditure objectives; and*
>
> *(iii) a realistic expectation of the demand forecast, cost inputs and other relevant inputs required to achieve the capital expenditure objectives*

Source: NER 6.5.7(c) Forecast capital expenditure, v230

Figure 1.3: NER capital expenditure objectives

> ***NER capital expenditure objectives***
>
> *(a) A building block proposal must include the total forecast capital expenditure for the relevant regulatory control period which the Distribution Network Service Provider considers is required in order to do each of the following* ***(the capital expenditure objectives****):*
>
> *(2) meet or manage the expected demand for standard control services over that period;*
>
> *(3) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;*
>
> *(4) to the extent that there is no applicable regulatory obligation or requirement in relation to:*
>
> *(i) the quality, reliability or security of supply of standard control services; or*
>
> *(ii) the reliability or security of the distribution system through the supply of standard control services,*
>
> *to the relevant extent:*
>
> *(iii) maintain the quality, reliability and security of supply of standard control services; and*
>
> *(iv) maintain the reliability and security of the distribution system through the supply of standard control services;*
>
> *(5) maintain the safety of the distribution system through the supply of standard control services; and*
>
> *(6) contribute to achieving emissions reduction targets through the supply of standard control services.*

Source: NER 6.5.7(a) Forecast capital expenditure, v230

Opex Objectives and Criteria

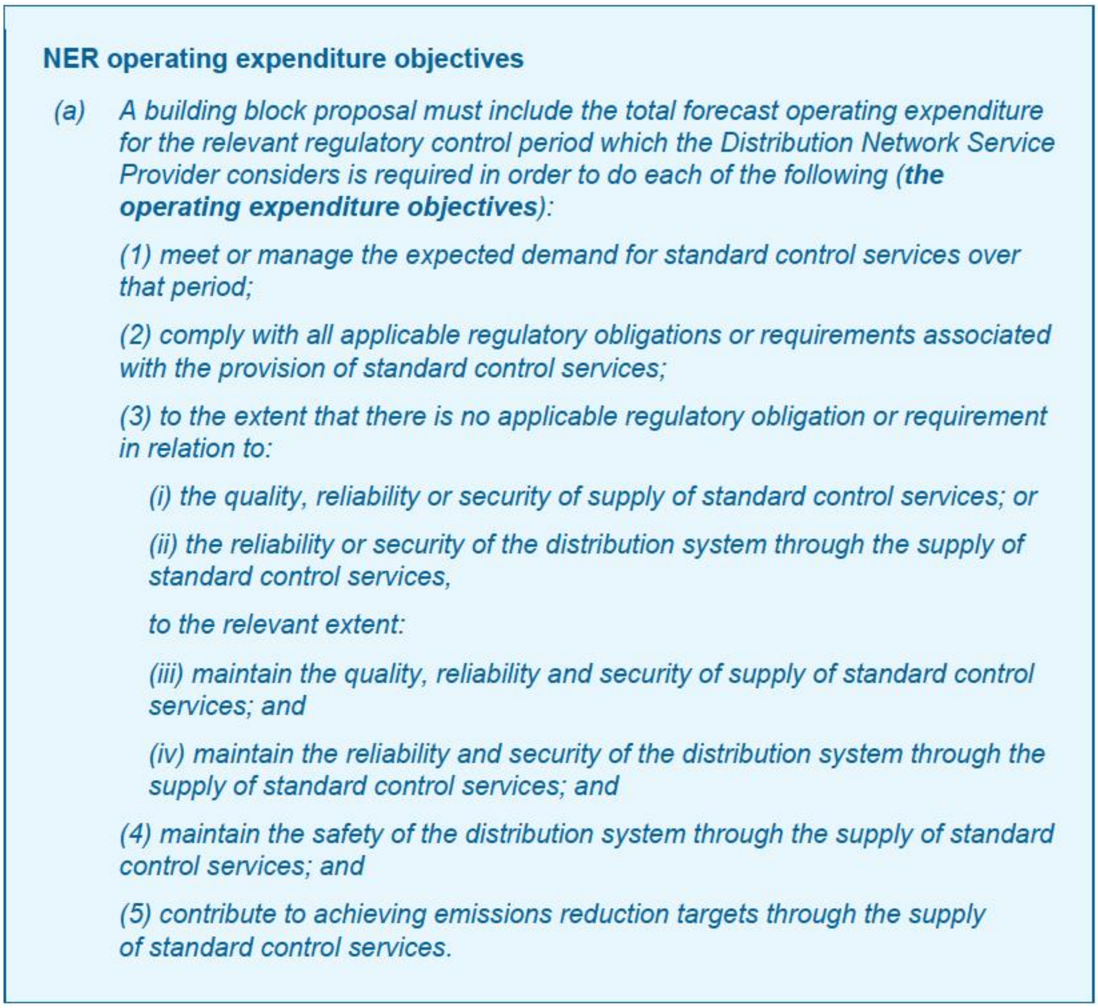
13. The most relevant aspects of the NER in this regard are the 'operating expenditure criteria' and the 'operating expenditure objectives.' The NER's opex criteria and opex objectives are reproduced below.

Figure 1.4: NER operating expenditure criteria

> **NER operating expenditure criteria**
>
> *(c) The AER must accept the forecast of required operating expenditure of a Distribution Network Service Provider that is included in a building block proposal if the AER is satisfied that the total of the forecast operating expenditure for the regulatory control period reasonably reflects each of the following (**the operating expenditure criteria**):*
>
> *(1) the efficient costs of achieving the operating expenditure objectives;*
>
> *(2) the costs that a prudent operator would require to achieve the operating expenditure objectives; and*
>
> *(3) a realistic expectation of the demand forecast, cost inputs and other relevant inputs required to achieve the operating expenditure objectives.*

Source: NER 6.5.6(c) Forecast operating expenditure, v230

Figure 1.5: NER operating expenditure objectives



NER operating expenditure objectives

*(a) A building block proposal must include the total forecast operating expenditure for the relevant regulatory control period which the Distribution Network Service Provider considers is required in order to do each of the following (**the operating expenditure objectives**):*

(1) meet or manage the expected demand for standard control services over that period;

(2) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;

(3) to the extent that there is no applicable regulatory obligation or requirement in relation to:

(i) the quality, reliability or security of supply of standard control services; or

(ii) the reliability or security of the distribution system through the supply of standard control services,

to the relevant extent:

(iii) maintain the quality, reliability and security of supply of standard control services; and

(iv) maintain the reliability and security of the distribution system through the supply of standard control services; and

(4) maintain the safety of the distribution system through the supply of standard control services; and

(5) contribute to achieving emissions reduction targets through the supply of standard control services.

Source: NER 6.5.6(a) Forecast operating expenditure, v230

How we have interpreted the capex criteria and objectives in our assessment

14. We have taken particular note of the following aspects of the capex criteria and objectives:

- Drawing on the wording of the first and second criteria, our findings refer to efficient and prudent expenditure. We interpret this as encompassing the extent to which the need for a project or program or opex item has been prudently established and the extent to which the proposed solution can be considered to be an appropriately justified and efficient means for meeting that need.
- The criteria require that the forecast '*reasonably reflects*' (emphasis added) the expenditure criteria and in the third criterion, we note the wording of a '*realistic expectation*'. In our review we have sought to allow for a margin as to what is considered reasonable and realistic, and we have formulated negative findings where we consider that a particular aspect is outside of those bounds.
- We note the wording '*meet or manage*' in the first objective (emphasis added), encompassing the need for the NSP to show that it has properly considered demand management and non-network options.
- We tend towards a strict interpretation of compliance (under the second objective), with the onus on the NSP to evidence specific compliance requirements rather than to infer them.
- We note the word '*maintain*' in objectives 3 and 4 and, accordingly, we have sought evidence that the NSP has demonstrated that it has properly assessed the proposed

expenditure as being required to reasonably maintain, as opposed to enhancing or diminishing, the aspects referred to in those objectives.

1.3.2 Technical review

15. Our assessments comprise a technical review. While we are aware of stakeholder inputs on aspects of what AusNet has proposed, our technical assessment framework is based on engineering considerations and economics.

16. We have sought to assess AusNet's expenditure proposal based on AusNet's analysis and AusNet's own assessment of technical requirements and economics and the analysis that it has provided to support its proposal. Our findings are therefore based on this supporting information and, to the extent that AusNet may subsequently provide additional information or a varied proposal, our assessment may differ from the findings presented in the current report.

17. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what AusNet has proposed and our assessment takes account of this range of information provided. To the extent that we found discrepancies in this information, our default position is to revert to AusNet's RP documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 This report

1.4.1 Report structure

18. In the following assessment section, we have presented:

- An overview of the proposed expenditure and a summary of AusNet's justification for that expenditure
- Our assessment of proposed cyber security expenditure, and
- Our findings for proposed cyber security expenditure and the implications of the findings for the expenditure allowances determined by the AER in its Draft Determination.

19. We also provide the following appendices:

- Appendix A - Cyber security background
- Appendix B - for relevant AER Guidelines.

20. We have taken as read the considerable volume of material and analysis that AusNet provided, and we have not sought to replicate this in our report except where we consider it to be directly relevant to our findings.

1.4.2 Information sources

21. We have examined relevant documents that AusNet has published and/or provided to the AER in support of the areas of focus and projects that the AER has designated for review. This included further information at onsite meetings and further documents in response to our information requests. These documents are referenced directly where they are relevant to our findings.

22. Except where specifically noted, this report was prepared based on information provided by AER staff prior to 30 May 2025 and any information provided subsequent to this time may not have been taken into account.

23. Unless otherwise stated, documents that we reference in this report are AusNet documents comprising its RP and including the various appendices and annexures to that proposal.

24. We also reference responses to information requests, using the format IRXX being the reference numbering applied by the AER. Noting the wider scope of the AER's

determination, the AER has provided us with IR documents that it considered to be relevant to our review.

1.4.3 Presentation of expenditure amounts

25. Expenditure is presented in this report in $2025-26 real terms, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.

26. While we have endeavoured to reconcile expenditure amounts presented in this report to source information, in some cases there may be discrepancies in source information provided to us and minor differences due to rounding. Any such discrepancies do not affect our findings.

2 REVIEW OF PROPOSED CYBER SECURITY EXPENDITURE

Common to its industry peers, AusNet's technology systems, applications and infrastructure are targets for cyber security threats. It has formed the reasonable position that the cyber threat risk will escalate over the course of the next RCP and it needs to invest in measures to strengthen its cyber security defences to mitigate the risk of a successful cyber breach.

We find that the AusNet group's proposed objective of achieving SP-3 cyber maturity as measured against the AESCSF by 2030 is appropriate given that it comprises gas and electricity distribution and electricity transmission businesses. AusNet electricity distribution benefits from the cyber defence, detection, and response capabilities from the combined enterprise approach, which proffers a higher security profile target than it might be able justify as a stand-alone business.

The aggregate investment at the group level is relatively high despite the scale economies that exist, but the quantum is explained satisfactorily by AusNet's risk and capability gap analysis and its relatively low current state maturity level.

We consider that the proposed capex is reasonable and that AusNet's proposed opex step change is a reasonable estimate of incremental opex that Ausnet will need to incur.

2.1 Introduction

27. In this section we assess the prudency and efficiency of AusNet's proposed expenditure to sustaining its current level of cyber security capability and to enhance it through the next RCP to address forecast continuing escalation of cyber threats.

28. AusNet's business case presents the costs for the standalone distribution business, however it represents a 25% allocation of the total proposed expenditure for the three AusNet group businesses (gas distribution. We differentiate between the reasonableness of the allocated versus the total, enterprise level costs where appropriate.

2.2 Background and context

29. In the appendix to this document, we provide background and context information on the cyber security threat landscape in Australia, relevant cyber security frameworks and obligations and their relevance to DNSPs.

30. In undertaking our assessment, we take account of the following factors.

Increasing threat landscape and attack surface mean cyber risk is increasing

31. The advice from government agencies is both that the cyber-attack landscape is worsening and that the cyber-attack surface presented by NSPs is increasing, leading to an increasingly higher risk of cyber-attack and potential breach.

32. In our assessment we have sought to understand how AusNet has incorporated the increasing threat landscape and attack surface issues into its risk analysis and, ultimately into its option selection and proposed expenditure profile.

Cyber security compliance obligations for NSPs are derived from the (amended) SOCI Act and from consideration of certain amendments to the Privacy Act

33. The minimum obligations for NSPs under the SOCI Act have been enhanced over the period FY22 and FY23 to include the following:

- Register of Critical Infrastructure Assets
- Mandatory Cyber Incident Reporting
- CIRMP, which requires completion of all the practices (and absence of anti-patterns) required to achieve SP-1 noting that SP-1 is the least onerous of the security profiles under the AESCSF.

34. [redacted]

35. Further the civil penalties for a breach(es) of the Privacy Act have been increased in 2022 from $2.2 million to $50.0 million (maximum) with the expectation from the Federal government via the amendment that organisations such as AusNet will act accordingly to undertake robust privacy and security practices which we interpret to include cyber security-related practices.

36. We have assessed how AusNet has responded to its common and specific cyber security compliance obligations, cognisant of:

- The worsening threat landscape and attack surface issues, and
- Its expected cyber security compliance position at the end of the current RCP.

37. We have also considered whether AusNet has identified any other relevant obligations.

38. In addition to its minimum compliance obligations, we consider the controls AusNet has proposed (and the cost of them) to manage the increasing cyber security threat landscape. A useful reference is the SP practices expected to be in place by the end of the current RCP and the projected SP practices it is likely to achieve with the proposed investment by the end of the next RCP.

2.3 Overview and summary of AusNet's proposed expenditure

2.3.1 What AusNet has proposed in its RP

39. AusNet's cybersecurity proposal for the next RCP is based on achieving SP-3 under version 2 of the AESCSF. As shown in Table 2.1, AusNet has proposed $27.5 million capex and $1.8 million opex step change in the next RCP to achieve and sustain this level of cyber security maturity.

40. AusNet advises that in accordance with its Cost Allocation Methodology, it has allocated 25% of the total cost to the electricity distribution business, so the totex in Table 2.1 is 25% of the totex for the three Ausnet businesses (i.e. electricity transmission and distribution, and gas distribution).[1]

41. The business case refers to $2024 and identifies capex split between recurrent and non-recurrent expenditure:[2]

- Recurrent investment of $16.2 million for lifecycle refreshes of its current cyber security systems and applications, and
- Non-recurrent investment of $8.7 million to uplift capabilities to achieve SP-3

[1] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 4

[2] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 20

42. AusNet's recurrent investment is designed to (i) maintain its current risk profile against SP-2 on the [then] current 2024 threat landscape, and (ii) provide the base layer from which to implement additional cyber security capabilities.

43. The additional cyber security capabilities required to achieve SP-3 are assessed by AusNet to minimise risk given the cyber threat landscape through to 2031.

Table 2.1: AusNet's proposed expenditure for cyber security - $m, real 2026

	2026	2027	2028	2029	2030	TOTAL
Capex	5.4	5.5	5.5	5.5	5.6	27.5
Opex step change	0.0	0.2	0.4	0.6	0.7	1.8
Total	**5.4**	**5.6**	**5.9**	**6.1**	**6.3**	**29.4**

Source: ASD EDPR 2026-31 – SCS Capex Model – 310125 and EMCa derived from AusNet model: ASD – AusNet – Accumulated Workbook for Opex and Step Changes – 31 Jan 2025

2.4 Assessment

2.4.1 AusNet's cyber security strategy and objectives

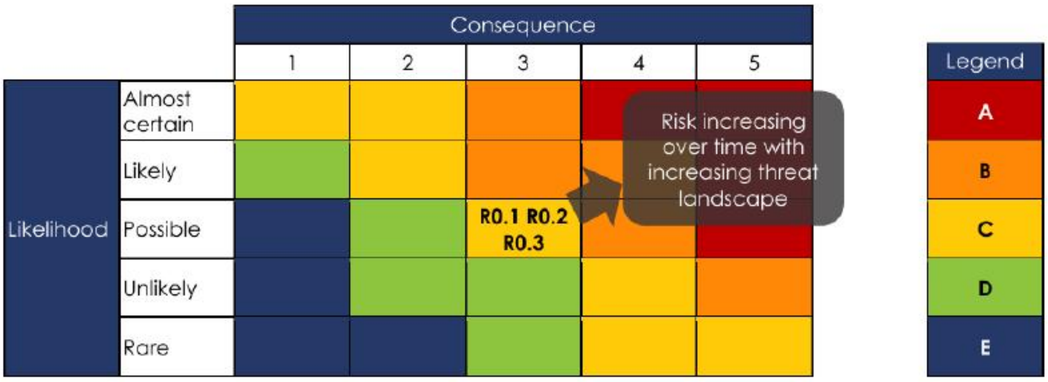
Increased cyber threat and compliance obligations are identified

44. In its business case, AusNet has adequately identified (i) its legislative obligations, (ii) the increasing threat landscape, and (iii) its increasing attack surface area, with the latter mainly attributed to the increasing interactions between AusNet's OT and customer energy resources.

45. Figure 2.2 illustrates AusNet's qualitative risk assessment against the three risk scenarios and represented here as R0.1, R0.2 and R0.3. Qualitatively, this risk assessment is consistent with the threat landscape (and increasing attack surface) and with other analyses we have seen undertaken by AusNet's peers.

46. This gives rise to a case for AusNet to consider investment to mitigate the risk increase.

Figure 2.1: AusNet's current state risk assessment



Source: ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, Figure 2

AusNet is on track to achieve SP-2 (v1) by the end of the current RCP

47. The AER's most recent determination for AusNet's Transmission Revenue Reset determined that SP-2 (V1) was an appropriate target. AusNet advises that it is on track to achieve this security profile by the end of the current RCP:

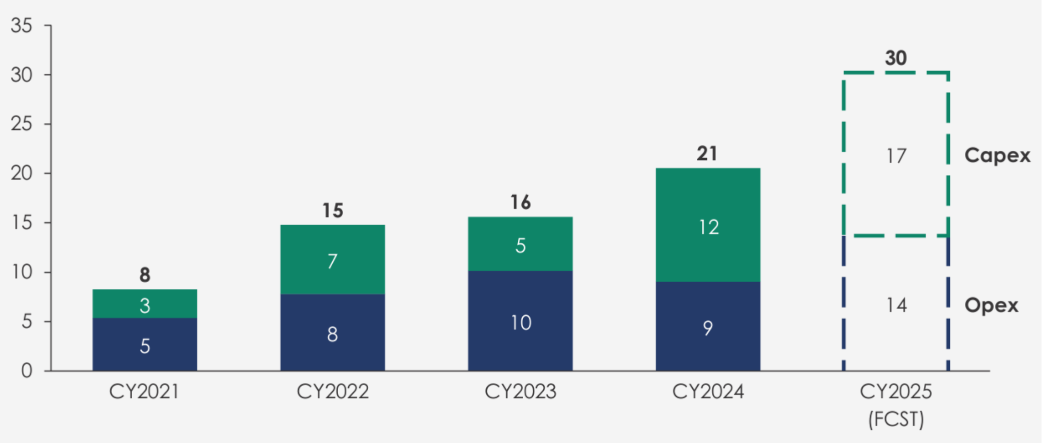
> *'As a multi-network business, with predominantly common and shared digital infrastructure, our cyber uplift initiatives apply across our transmission and distribution networks.'*[3]

48. As a result:

- Cyber security capabilities for the electricity distribution network are also expected to reach SP-2 (V1) by the end of the 2021-26 RCP, and
- The distribution network is forecast to bear 25% of the total expenditure of shared cyber security expenditure.

49. Commensurate with the increase in cyber security breaches in Australia and internationally, and the AER's determination, AusNet has been building its cyber security capability over the current RCP. As shown in Figure 2.2, AusNet's cyber security investment has been increasing rapidly as it aligns its cyber practices with AESCSF (v1) SP-2 requirements.

Figure 2.2: AusNet annual cyber security expenditure in the current RCP (m)



Source: On-site Day 3, slide 45

AusNet's response to compliance obligations and increasing cyber security risk in the next RCP is to achieve SP-3

50. Recent risk assessment commenced by an external third-party provider identified material risks that are outside AusNet's appetite. Due to evolving regulations and sophisticated cyber-attacks, SOCI's current framework may not be suitable for 2030, stating that:

> *'AusNet is committed to adhering to key regulatory acts and transitioning from a compliance-led approach to a more robust, risk-based program utilising AESCSF (v2) framework.'*[4]

51. As shown in Figure 2.3 is to achieve AESCSF V2 SP-3 maturity by the end of the next RCP. AusNet argues that as an operator of critical infrastructure in the form of transmission and distribution networks, it has an obligation under the AESCSF to achieve this level of maturity.[5]

[3] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 5

[4] AusNet EDPR Onsite Workshop - Day 3 Pack CONF, slide 42

[5] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 20

[redacted]

AusNet proposes to invest to *maintain* risk across three dimensions at an acceptable level

52. AusNet's position regarding cyber security is enunciated in the following quote from its business case:[6]

> *'AusNet is risk averse in our approach to preventing cyber security events. We adopt a 'so far as is reasonably practical' approach. This involves regularly assessing the macro-environment and receiving intelligence from Government on risk levels and vulnerabilities.'*

53. To enact this position, AusNet has adopted a strategy that is now common in the industry of undertaking a risk-based analysis and to invest in maintaining current levels of risk across the three risk scenarios it has focussed on:

- Compromised operation of the network
- Compromised data, and
- Compromised staff operations.

54. These risk scenarios are commonly applied in the industry as part of their respective risk analyses.

55. AusNet claims that as a combined Transmission and distribution provider it must meet the *'highest requirement of the market roles it plays'*[7] with reference to Figure A.1 (AESCSF criticality bands). We consider this to be a reasonable interpretation of AEMOs guidance, noting that AusNet correctly observes that there is no mandatory requirement associated with the AESCSF. Hence a risk-based approach is appropriate, rather than a compliance-driven strategy, in our view.

AusNet's security operations center is based on a hybrid delivery model which is common industry practice

56. AusNet has adopted a hybrid strategy for its Security Operations Center (SOC), with a relatively small team of internal resources [redacted] Figure 2.4. Whilst a hybrid strategy is common in the industry, in our experience most utilities have a higher number of in-house resources, reducing reliance on external service providers. Whilst inherently there is no 'right model', we explored the approach with AusNet at the on-site meeting noting its comment that '*the current Security Operations Centre is legacy and is reducing the effectiveness of our threat detection and response capability…'* [8] AusNet advised that as part of its preferred option, it would invest to strengthen the threat detection and response capability overseen by the SOC.

57. The list of contributing issues with its current SOC are compelling for the mooted improvements to threat detection and response.

[6] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 10

[7] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 10

[8] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 16

[redacted]

- [redacted]

2.4.2 AusNet's cyber security systems refresh program

63. We first assess AusNet's proposed refresh (or recurrent) cyber security expenditure, for which the objective is to maintain its existing cyber security and IT resilience capabilities.

Overview of options

64. AusNet presents only two options, as shown in Table 2.2. The cost of Option 1 is not presented in the business case.

Table 2.2: Cyber security recurrent expenditure options considered by AusNet

Option	Description
1. Actively manage without vendor support	*Operate control, metering and business systems without performing updates, patching or refreshes and actively manage the risks in-house*
2. Perform lifecycle refreshes (recommended)	*Where prudent and efficient, performing refreshes, upgrades and patching of cyber security systems in line with vendor recommendations and maintaining vendor support*

Source: ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, Table 3

Option 1 is not representative of good industry practice

65. AusNet's rationale for not selecting Option 1 is based largely on qualitative risk analysis, and is summarised as, *'[w]ithout vendor support it is likely there will be more unpatched cyber security systems with vulnerabilities, which will see our cyber security environment degrade relative to current capabilities and risk levels.'* AusNet does acknowledge that the risk could be offset to some extent by additional support / monitoring at an additional (unspecified cost).

66. The lack of detail makes comparative analysis more challenging than it needs to be however, in our experience:

- More than one-to-two years of deferral of patching (least cost), refreshes, and updates (highest cost) of the applications and systems supporting cyber security at AusNet would progressively reduce the maturity level, and
- Given the nature of AusNet's business (i.e. critical infrastructure transmission and distribution), not maintaining at least SP-2 would not be consistent with the actions of a prudent operator.

Option 2 is consistent with good industry practice

67. AusNet has identified the 'SP-2 V1' systems and applications that require 'refresh' during the next RCP, including a table which identifies six areas of investment[9] encompassing a variety of security applications, app firewalls, perimeter firewalls, security information, and event management tools, with the aggregate cost for each of the six areas.[10]

68. The proposed $16.2 million capex ($2024) is only to maintain the capabilities of the systems, applications, platforms, practices and capability more generally that it will have established by the end of the current RCP (i.e. SP-2 V1).

69. We consider that (i) it is reasonable for AusNet to state that it will achieve SP-2 V1 by the end of the next RCP, (ii) if it does not retain the currency of the underpinning capabilities throughout the next RCP, its cyber risk level would gradually escalate, and (iii) this would not be consistent with good industry practice given the escalating threat landscape and attack surface faced by the electricity sector.

Option 2 cost is reasonably derived

70. AusNet advises that the refresh cycles that it intends to follow are in line with vendor recommendations' and that the cost estimates are based on (i) vendor engagement, and (ii) benchmarks from recent projects and industry standards.[11]

71. We explored both of these claims at the onsite meeting. We usually consider that following vendor refresh timing recommendations even for more significant IT system, apps, and infrastructure is unnecessarily conservative. However, in the case of capability directly

[9] Patching: Infrastructure and Application security and vulnerability; Refresh: Network security (OT and IT), Security assets (IT and OT), Governance, Risk and Compliance platform

[10] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, Table 2

[11] AusNet EDPR Onsite Workshop – Day 3 Pack CONF, slide 47

related to cyber security, we consider it more likely to be prudent to keep up to date in accordance with the vendor recommendations.

72. With respect to the proposed cost of the proposed patches and refreshes, based on AusNet's responses and our own experience in evaluating similar DNSP proposals, we are satisfied that the aggregate cost is representative of a reasonable estimate.

2.4.3 AusNet's cyber security new threat/capability uplift program

AusNet considered two options to achieve an acceptable risk level by the end of the next RCP

73. AusNet's identified need for investment in cyber security capability uplift is to respond to the increased risk of cyber-attacks, AusNet's risk tolerance, and recent successful cyber-attacks (and the cost and reaction to them by customers). It identified two credible options, described in Table 2.3.[12]

Table 2.3: Cyber security non-recurrent expenditure options considered by AusNet ($2024)

Option	Cost
1. Achieve AESCSF V2 SP-2	$6.8 million (distribution network only)
2. Achieve AESCSF V2 SP-3	$8.7 million (distribution network only)

Source: ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, Table 5

74. AusNet also discusses two other options which it labels 'non-credible'. The first is to develop a standalone approach to uplifting cyber security for the distribution network only. The second was to align its cyber security to AESCSF V1. For reasons explained in its business case, we see no merit in pursuing these options.

75. AusNet's qualitative risk analysis that achieving SP-2 V2 would likely see an increase in cyber security risk over the next RCP is consistent with similar assessments by their peers, with the highest residual risk being 'possible' compromise to network operation with 'major' impact to customers. The other two risk scenarios (compromised data and compromised staff operations) were assessed by AusNet as level C which we assume from its analysis of its preferred option is tolerable.

76. AusNet's preferred option to address all the gaps between its projected SP-2 V1 maturity level at the end of the current RCP and SP-3 V2, as described in its business case. It assesses the latter (qualitatively) to maintain the risk level as tolerable (level 'C', which in this case is a likelihood of 'possible' with a consequence of 'severe' impact).[13]

If not for the small cost difference between Options 1 and 2 another option should have been considered

77. Other DNSPs have typically selected an option based on implementing the necessary controls to achieve all the SP-2 V2 practices and selected, high value SP-3 V2 practices. The option focusses on maximising risk reduction on a value-for-money basis whilst seeking to end up with the risk level at the end of the period the same as at the start. This approach by other NSPs has typically resulted in 80-90% of SP-3 practices being targeted with a 5%-10% lower cost, for minimum additional risk. However, given that the cost differential between Options 1 and 2 is surprisingly small at $1.9 million ($2024) *for the distribution business only*,[14] we can understand the omission of the option.

[12] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, page 15

[13] ASD - AusNet - Digital Business Case - Cyber security - 310125 – CONF, Figures 5 and 6

[14] As the DNSP is allocated only 25% of the total cost, the margin between Options 1 and 2 for the business as a whole is more significant, but is still relatively narrow

AusNet has not provided a quantified cost-benefit analysis to help demonstrate the prudency of its proposed non-recurrent ICT expenditure

78. Our understanding is that AusNet's proposed investment is to enhance cyber security capability to maintain the risk level from the start of the next RCP to the end. Arguably the non-recurrent expenditure could be classified as 'Maintaining existing services, functionalities, capability and/or market benefits.'[15] However, NSPs typically demonstrate that benefits exceed the costs of implementing the new/expanded cyber security capability through quantified cost-benefit analysis, in accordance with AER's expectations for the sub-category of 'New or expanded ICT capability, functions and services.'[16] Regardless, it is expected by the AER that a cost-benefit analysis is undertaken to help demonstrate the prudency of the selected option.

79. AusNet has chosen not to present a cost-benefit analysis to demonstrate the prudency of its selected option, instead relying on qualitative risk analysis to comparing the two identified options. This is not consistent with good industry practice nor the AER's guideline.

The cost estimate for implementing the non-recurrent capability uplift is reasonably derived

80. AusNet has identified eight programs to implement the controls and practices to address the gaps between SP-2 (V1) and SP-3 (V2) and has provided the cost estimates for each. The programs (or suite of initiatives) cover controls that are typical of industry responses to enhance cyber security resilience, including zero trust architecture, AI/machine learning, OT/IOT, cloud security, and threat detection and response.

81. As with the recurrent cost estimates, AusNet advises that the non-recurrent estimates were based on vendor engagement and benchmarks from recent projects and industry standards. This is an acceptable approach when matched to the level of detail provided about each initiative, although we note that this can lead to a degree of bias.

Despite the absence of a NPV analysis we consider Option 2 to be the prudent choice

82. Given the relatively narrow margin between Options 1 and 2, and the reasonableness of AusNet's qualitative risk assessment (which can be translated to a benefit from avoided risk), we are satisfied that Option 2 (achieving SP-3) is the prudent approach.

2.5 Summary of our findings and implications for AusNet's proposed cyber security expenditure

2.5.1 Summary of our findings

83. We consider that the proposed capex and opex is reasonable.

84. We are satisfied that it is prudent for AusNet to invest in maintaining its cyber security risk level at a tolerable level in the face of an escalating threat landscape and attack surface.

85. Given the scope of the AusNet Group businesses (gas and electricity – transmission and distribution) we are satisfied that the strategy of targeting SP-3 level of maturity against the AESCSF by 2030 and sustaining it is appropriate.

86. The total cost of the two preferred cybersecurity options proposed by AusNet and attributable to the distribution network is $27.5 million, which equates to a total cost of $110 million to the combined transmission, gas and electricity distribution networks. This is commensurate with the highest level of cybersecurity expenditure amongst its peers. However, we are cognisant that this cost is to achieve SP-3 maturity across three significant businesses and to sustain it.

[15] Refer to the sub-categories of non-recurrent ICT expenditure in Appendix B

[16] Refer to Appendix B

2.5.2 Implications for proposed capex and opex step change allowances

87. We consider that AusNet’s proposed capex is reasonable and that AusNet’s proposed opex step change is a reasonable estimate of incremental opex that Ausnet will need to incur.

APPENDIX A – CYBER SECURITY BACKGROUND AND CONTEXT INFORMATION

A.1 Cyber security threat in Australia

Increasing threat level is reported by the ACSC

88. The Australian Signal Directorate's (ASD) Australian Cyber Security Centre ('ACSC') monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2023-24) it states that: '*In FY2023-24, ASD received over 36,700 calls to its Australian Cyber Security Hotline, an increase of 12% from the previous financial year. ASD also responded to over 1,100 cyber security incidents, highlighting the continued exploitation of Australian systems and ongoing threat to our critical networks.'*[17]

There is an increasing cyber threat against critical infrastructure

89. State actors are focussed on critical infrastructure worldwide

90. The Australian Signals Directorate (ASD) states:

> *'State-sponsored cyber actors persistently target Australian governments, critical infrastructure and businesses using evolving tradecraft. These actors conduct cyber operations in pursuit of state goals, including for espionage, in exerting malign influence, interference and coercion, and in seeking to pre-position on networks for disruptive cyber attacks.*[18]

91. Australian critical infrastructure has been targeted:[19]

> *'Critical infrastructure networks are an attractive target due to the sensitive data they hold and the widespread disruption that a cyber security incident can cause on those networks. In FY2023-24, over 11% of cyber security incidents ASD responded to related to critical infrastructure. Compromise could lead to the disruption of critical services, affecting the economy and lives of everyday Australians.'*

92. The 2024 Report further states that: '*Operational technology systems are increasingly interconnected and can have vulnerabilities that make them an easier cyber target. Secure information and communications technology and operational technology systems are necessary to protect Australia's critical services.'*[20]

93. The ASD advises that: '*Critical infrastructure organisations should adopt a stance of `when' not `if' a cyber security incident will occur.'*[21]

A.2 Critical infrastructure regulation

A.2.1 Amendments to the SOCI Act

[17] ASD Cyber Threat Report 2023-24. Executive Summary

[18] ASD Cyber Threat Report 2023-24. Executive Summary

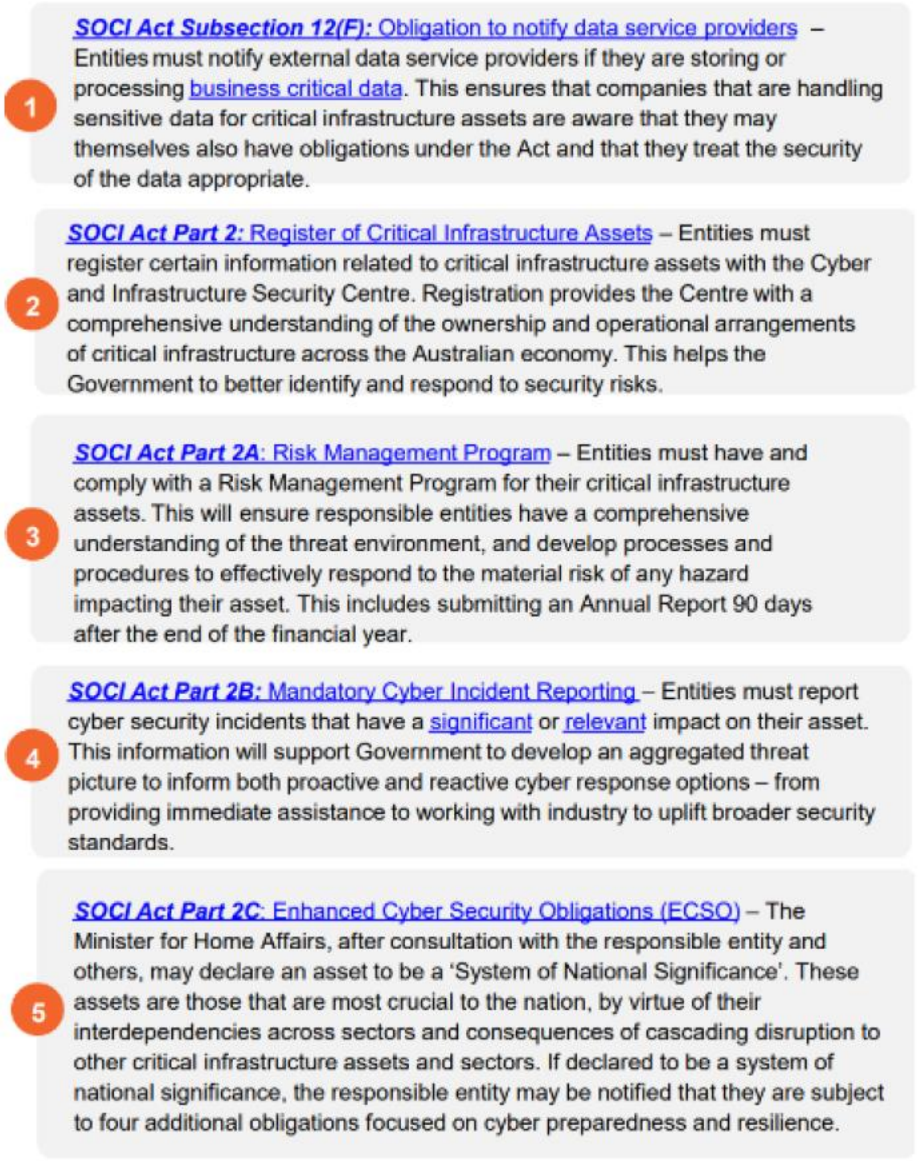
[19] ASD Cyber Threat Report 2023-24. Executive Summary

[20] ASD Cyber Threat Report 2023-24. Chapter 2

[21] ASD Cyber Threat Report 2023-24. Chapter 2

94. The Security of Critical Infrastructure Act 2018 (SOCI Act) places obligations on specific entities in the electricity industry. It was amended in 2021 and 2022 to more appropriately capture those assets that are critical to Australia's defence, national security, economy and social stability. It was further amended in 2024 by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (ERP Act) in response to significant incidents impacting critical infrastructure. The objectives of the amendments were to lift existing obligations for responsible entities under the Act and to enhance the government's ability to manage the consequences of all hazardous incidents on critical infrastructure assets.[22] Figure A.1 summarises the relevant obligations.

Figure A.1: Obligations for responsible entities under the SOCI Act



1 ***SOCI Act Subsection 12(F):*** Obligation to notify data service providers – Entities must notify external data service providers if they are storing or processing business critical data. This ensures that companies that are handling sensitive data for critical infrastructure assets are aware that they may themselves also have obligations under the Act and that they treat the security of the data appropriate.

2 ***SOCI Act Part 2:*** Register of Critical Infrastructure Assets – Entities must register certain information related to critical infrastructure assets with the Cyber and Infrastructure Security Centre. Registration provides the Centre with a comprehensive understanding of the ownership and operational arrangements of critical infrastructure across the Australian economy. This helps the Government to better identify and respond to security risks.

3 ***SOCI Act Part 2A***: Risk Management Program – Entities must have and comply with a Risk Management Program for their critical infrastructure assets. This will ensure responsible entities have a comprehensive understanding of the threat environment, and develop processes and procedures to effectively respond to the material risk of any hazard impacting their asset. This includes submitting an Annual Report 90 days after the end of the financial year.

4 ***SOCI Act Part 2B:*** Mandatory Cyber Incident Reporting – Entities must report cyber security incidents that have a significant or relevant impact on their asset. This information will support Government to develop an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance to working with industry to uplift broader security standards.

5 ***SOCI Act Part 2C***: Enhanced Cyber Security Obligations (ECSO) – The Minister for Home Affairs, after consultation with the responsible entity and others, may declare an asset to be a 'System of National Significance'. These assets are those that are most crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors. If declared to be a system of national significance, the responsible entity may be notified that they are subject to four additional obligations focused on cyber preparedness and resilience.

Source: https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf

95. [redacted]

[22] [redacted]

[redacted]

A.2.2 CIRMP - AESCSF Security Profile 1 and Essential Eight Maturity Model

96. Under the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023, a responsible entity must establish and maintain a process or system in the CIRMP to (a) comply with a framework contained in one of five documents referred to in the CIRMP, and (b) meet the corresponding condition for that document.[24] The CIRMP must be in place within 18 months of the commencement of the instrument or within 18 months of the asset being designated a critical (electricity) infrastructure asset.[25]

97. The 2020-21 AESCSF Framework Core published by AEMO is one of the five documents referred to in the CIRMP instrument and the condition that is required to be met is SP-1. Therefore SP-1 is the legislative obligation that Network Service Providers (NSPs) must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.

98. Equally, the *Essential Eight Maturity Model* (EEMM) published by the Australian Signals Directorate is another referenced framework and the condition if it is adopted by an NSP is meeting Maturity Indicator Level one (MIL-1). Therefore MIL-1 is the legislative obligation to which NSPs must comply with if the NSP is defined as a responsible entity and the NSP selects the EEMM as its cyber security framework.

Privacy Act amendments 2022[26]

99. The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill) amends the Privacy Act 1988 to expand the Australian Information Commissioner's enforcement and information sharing powers, and to increase penalties for serious or repeated interferences with privacy.

100. The Bill increases the maximum penalty under section 13G of the Privacy Act for a body corporate to an amount not exceeding the greater of $50 million, three times the value of the benefit obtained or, if the court cannot determine the value of the benefit, 30% of their adjusted turnover in the relevant period. The maximum penalty of $50 million is an increase from the pre-existing maximum of $2.2 million.

101. Within the Explanatory Memorandum to the Bill, it is stated that '[b]y strengthening penalties, Australia will be signalling its expectations that businesses undertake robust privacy and security practices.'[27]

A.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

A.3.1 AESCSF V1

102. In response to the Finkel National Electricity Market Review recommendation 2.10 in 2018, the Australian Energy Market Operator (AEMO) collaborated with industry and government to develop the AESCSF. Among other markets, it covers Australia's electricity sector and is

[23] https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf

[24] Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 8 (4).

[25] Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 4(2) and subsection 8(3).

[26] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6940.

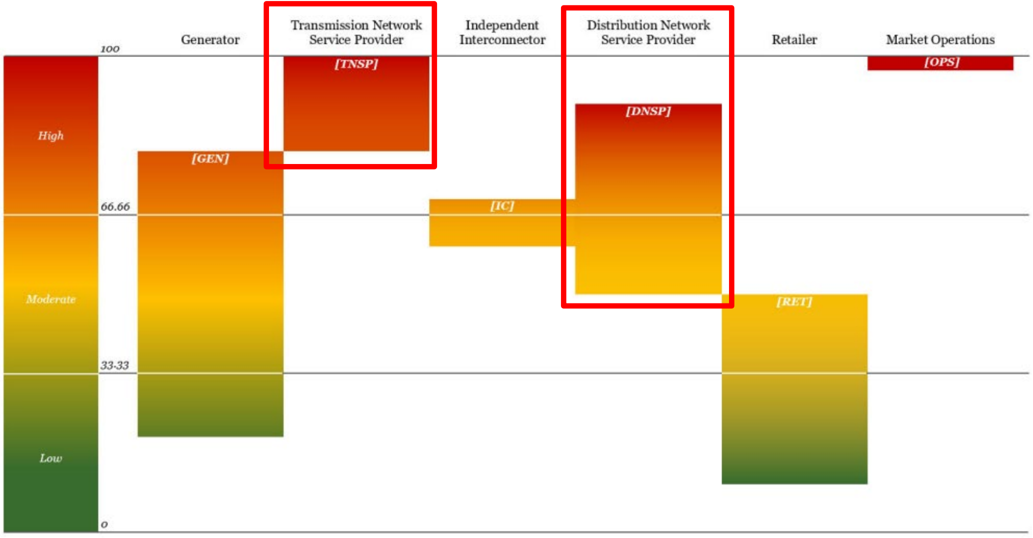
[27] Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 EXPLANATORY MEMORANDUM, in reference to Section 13G – civil penalties (para 12).

voluntary but has been adopted by NSPs.[28] The AESCSF Version 1 (V1) is divided into 11 domains, ten C2M2[29] domains, and the Australian Privacy Management Domain. There were minor revisions to the AESCSF in 2019, 2021, and 2022, with no significant changes in version 2022 compared to version 2021.[30] AESCSF V1 encompasses the 2018 and subsequent iterations up to and including the 2022 revision.

103. The AESCSF V1 program includes the Electricity Criticality Assessment Tool (E-CAT), which is designed to assess the relative criticality of NSPs and other participants in the electricity sector.

104. The E-CAT allows assessment of the relative criticality of entities participating in the electricity and other energy sectors. The diagram below represents the criticality banding for the electricity sub-sector only, with DNSP criticality rating ranging between the High and Medium bands.

Figure A.2: AESCSF E-CAT criticality bands for electricity sector – DNSPs highlighted



Source: AEMO, AESCSF Electricity Criticality Assessment Tool (E-CAT), per AESCSF V1

A.3.2 AESCSF Version 2 (V2)

105. In December 2022, Energy Ministers endorsed AESCSF V2, providing guidance about the continued role of the program to support energy sector cyber uplift and increasing cyber security requirements for the energy sector in line with escalating and evolving cyber threats.

106. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting CIRMP minimum obligations), and a transition plan to 'sunset' AESCSF V1. AESCSF V2 was released in 2023. The update to AESCSF v2 has resulted in an additional 72 practices (i.e., 20% additional practices). A summary of the difference between AESCSF V1 and V2 is summarised in v2.1 and AESCSF v2 is provided below. AEMO has stated previously that '*[t]he CAT should be treated as general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.*'[31]

[28] AEMO, AESCSF Framework and Resources, AEMO website.

[29] United States Department of Energy Cyber Security Capability Maturity Model.

[30] AEMO AESCSF Framework Overview – 2022 Program. Page 1.

[31] AEMO AESCSF Framework Overview – 2022 Program. Page 3.

Table A.1: AESCSF Version 1 and Version 2 comparison – Security Profiles

Security Profile	Participant criticality	Total practices/anti-patterns required to achieve SP	
		AESCSF V1	AESCSF V2
SP-1	Low	88	123
SP-2	Medium	200 (88+112)	275 (123+152)
SP-3	High	282 (200+82)	354 (278+79)

Source: AEMO, AESCSF V2 Summary of Changes, page 4

107. To help organisations define roadmaps to improved cyber security maturity, the ACSC includes guidance on 'Priority Practices' within each SP. The Priority Practices are recommended for completion first as part of any uplift program.

APPENDIX B - RELEVANT AER GUIDELINES FOR ASSESSMENT OF ICT EXPENDITURE

B.1 AER Guidelines for non-network ICT assessment

B.1.1 Assessment of non-network ICT capex

108. The scope of our assessment includes ex ante cyber security and ADMS capex, which are categorised as non-network ICT.

109. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to AusNet's proposed cyber security capex. The proposed expenditure is also 'non-recurrent'.

110. The AER requires DNSPs to allocate their non-recurrent ICT expenditures into the three subcategories for which it applies different assessment approaches, as described below:[32]

Maintaining existing services, functionalities, capability and/or market benefits

111. The AER states that:

> *Given that these expenditures are related to maintaining existing service, we note that it will not always be the case that the investment will have a positive NPV. As such, it is reasonable to choose the least negative NPV option from a range of feasible options including the counterfactual.' [33] We consider that such investments should be justified on the basis of a business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency). The assessment methodology would also give regard to the past expenditure in this subcategory.*[34]

Complying with new / altered regulatory obligations / requirements

112. The AER states that:

> *It is likely that for such investments, the costs will exceed the measurable benefits and as such, the least cost option will likely be reasonably acceptable in regard to the NER expenditure criteria. Therefore the assessment of these expenditures is similar to subcategory one. Should there be options to achieve compliance through the use of external service provides [sic], the costs and merits of these should be compared.'*[35]

New or expanded ICT capability, functions and services

113. The AER states that:

> *We consider that these expenditures require justification through demonstrating benefits exceed costs (positive NPV). We will make our assessment therefore through assessing the cost-benefit analysis. Where benefits exceed costs consideration should also be given to self-funding of the investment.*

[32] In cases where programs/projects cover multiple categories of expenditure, the distributor is expected to apportion costs from individual components across multiple categories to reflect the nature of the work undertaken.

[33] The only exception will be where the business can demonstrate that any unquantified/intangible benefits of an option can support the decision to not choose the highest NPV option.

[34] AER, Non-network ICT capex assessment approach, November 2019. Page 11.

[35] AER, Non-network ICT capex assessment approach, November 2019. Page 11.

> *For each subcategory of non-recurrent expenditure, we note that there may be cases where the highest NPV option is not chosen. In these cases, where either the chosen option achieves benefits that are qualitative or intangible, we would expect evidence to support the qualitative assumptions. We consider the evidence provided must be commensurate with the cost difference between the chosen and highest NPV option.*
>
> *We also note that where non-recurrent projects either lead to or become recurrent expenditures in the future, this needs to be identified in the supporting business case and accounted for in any financial analysis undertaken to support the investment.*[36]

B.1.2 Assessment of opex step changes

114. Our scope includes assessment of Jemena's proposed cyber security opex step changes. Section 2.2 of the AER's Expenditure Forecast Assessment Guideline for Electricity Distribution outlines its general approach for assessing opex step changes and which we have followed. In summary:

- The AER separately assesses the prudency and efficiency of forecast cost increases or decreases from new regulatory obligations and capex/opex trade-offs;
- For capex/opex trade-off step changes, the emphasis is on establishing whether it is prudent and efficient to substitute opex for capex; and
- For step changes arising from new regulatory obligations, the emphasis is on:
  - whether there is a binding change in regulatory obligations that affects the efficient forecast opex and when the change occurred, and
  - what options were considered and whether the selected option is an efficient option.[37]

[36] AER, Non-network ICT capex assessment approach, November 2019. Page 12.

[37] AER, Expenditure Forecast Assessment Guideline for Electricity Distribution. Page 11.