EMC[a]

energy market consulting associates

Endeavour Energy 2024 to 2029 Regulatory Proposal

REVIEW OF PROPOSED EXPENDITURE ON ICT CYBER SECURITY

Report prepared for:

AUSTRALIAN ENERGY REGULATOR

August 2023

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 Endeavour Energy from 1st July 2024 to 30th June 2029. 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 Endeavour Energy. 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 1st July 2023 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 Endeavour Energy'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 and Paul Sell with input Cesare Tizi and Eddie Syadan

Date saved
26/09/2023 3:43 PM

Version
Final v4

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
Level 1, 2 Mill Street, 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
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	The Australian Energy Sector Cyber Security Framework
Capex	Capital expenditure
CIRMP	Critical Infrastructure Risk Management Program
CISC	Critical Infrastructure Centre
Current RCP	FY20-FY24
DCCEEW	Department of Climate Change, Energy, the Environment and Water
DNSP	Distribution Network Service Provider
E-CAT	Electricity Criticality Assessment Tool
ECSO	Enhanced Cyber Security Obligations
EEMM	Essential Eight Maturity Model
FY	Financial Year
ICT	Information and Communication Technology
IT	Information Technology
MIL	Maturity Indicator Level
NER	National Electricity Rules
Next RCP	FY25-FY29
RCP	Regulatory Control Period
NPC	Net Present Cost
NPV	Net Present Value
NSP	Network Service Provider
NSW	New South Wales
Opex	Operating expenditure
OT	Operational Technology
RMP	Risk Management Plan
RP	Revenue Proposal
SLACI Act	Security Legislation Amendment Critical Infrastructure Act
SLACIP Act	Security Legislation Amendment Critical Infrastructure Protection Act
SOCI Act	Security of Critical Infrastructure Act
SoNS	Systems of National Significance

Term	Definition
SP	Security profile
TNSP	Transmission Network Service Provider

1 INTRODUCTION

AER has asked us to review and provide advice on Endeavour Energy's proposed allowance for cyber security-related expenditure in the next Regulatory Control Period. Our review is based on information that Endeavour Energy provided and on aspects of the National Electricity Rules relevant to assessment of expenditure allowances.

1.1 Objective of this report

1. In January 2023, Endeavour Energy submitted its Revenue Proposal (RP) for the next Regulatory Control Period 2024-29 ('next RCP') to the AER.
2. The purpose of this report is to provide the AER with a technical review of Endeavour Energy's proposed cyber security-related capital expenditure ('capex') and step-change operating expenditure ('opex') included in Endeavour Energy's Revenue Proposal ('RP') for the Regulatory Control Period 2024-29 ('next RCP').
3. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex and opex allowance as an input to its Draft Determination on Endeavour Energy's revenue requirements for the next RCP.

1.2 Scope of requested work

4. The scope of this review covers Endeavour Energy's proposed allowance for:
   - Non-recurrent ICT cyber security capex; and
   - An opex step change for ICT cyber security.
5. In preparing our findings, we are required to have regard to the AER's role under s.6 of the NER and the AER's forecast assessment guidelines.

1.3 Our review approach

6. In undertaking our review, we:
   - Completed a desktop review of the information provided to us by the AER followed by preparing requests for information to Endeavour Energy to help ensure that we correctly understood the methodology and assumptions that Endeavour Energy had applied in estimating its expenditure requirements;
   - Completed an assessment of relevant aspects of the expenditure forecast, including by taking into account the responses from Endeavour Energy to information requests; and
   - Documented our findings in this report.
7. We also provided feedback to AER staff on our preliminary findings in a teleconference, while drafting this report.
8. Our review considers the requirements of the National Electricity Rules (NER), specifically the capex and opex criteria and objectives, and the AER's expenditure assessment guideline.
9. Where we find that Endeavour Energy's forecast expenditure is not reasonable in terms of the relevant requirements of the NER, we have identified the extent to which the issues we have found have resulted in a higher level of expenditure than what would be required of a prudent and efficient service provider.

10. The limited nature of our review does not extend to advising on all options and alternatives that may be reasonably considered by Endeavour Energy, nor on all parts of its capex forecast or its proposed opex step change. To the extent that there may be implications for aspects of Endeavour Energy's RP that are beyond our scope, we have included additional observations in some areas that we trust may assist the AER with its own assessment.

1.3.1 Conformance with NER requirements

11. 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.

Capex and Opex objectives and criteria

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

13. The NER's capex criteria and capex objectives are reproduced in Figure 1.1 and Figure 1.2.

Figure 1.1: 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 and cost inputs required to achieve the capital expenditure objectives.

Source: NER 6.5.7(c) Forecast capital expenditure, v200

Figure 1.2: 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 achieve each of the following (**the capital 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.

Source: NER 6.5.7(a) Forecast capital expenditure, v200

14. The NER's opex criteria and opex criteria are reproduced in Figure 1.3 and Figure 1.4.

Figure 1.3: NER operational 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; and

(2) the costs that a prudent operator would require to achieve the operating expenditure objectives; and

(3) a realistic expectation of the demand forecast and cost inputs required to achieve the operating expenditure objectives

Source: NER 6.5.6 (c) Forecast operating expenditure

Figure 1.4: 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 achieve 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.

Source: NER 6.5.6 (a) Forecast operating expenditure

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

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

- Drawing on the wording of the first and second capex and opex 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 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 capex and opex criteria require that the forecast '*reasonably reflects*' the expenditure criteria and in the third criterion, we note the wording of a '*realistic expectation*' (emphasis added). 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 capex and opex objective (emphasis added), encompassing the expected demand for standard control services over the next RCP;
- We tend towards a strict interpretation of compliance (under the second capex and opex objective), with the onus on the NSP to evidence specific compliance requirements rather than to infer them; and
- We note the word '*maintain*' in capex and opex objectives 3 and 4. Depending on the context, 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.

16. The DNSPs subject to our review have applied a Base Step Trend approach in forecasting their aggregate opex requirements. Since our review scope encompasses only proposed expenditure for certain purposes, we have sought to identify where the DNSP has proposed an opex step change that is relevant to a component that we have been asked to review. Where the DNSP has not proposed a relevant opex step change, then we assume that any opex referred to in documentation that the DNSP has provided is effectively absorbed and need not be considered in our assessment.

1.3.2 Technical review

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

18. We have sought to assess Endeavour Energy's expenditure proposal based on Endeavour Energy's analysis and Endeavour Energy'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 Endeavour Energy may subsequently provide additional information or a varied proposal, our assessment may differ from the findings presented in the current report.

19. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what Endeavour Energy 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 Endeavour Energy regulatory submission documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 About this report

1.4.1 Report structure

20. The following sections of our report are structured as follows:

- In section 2, we present relevant context to our assessment including contextual information on cyber security threat to Australian electricity networks, regulation relevant to critical infrastructure, the relevant assessment framework and relevant regulatory guidelines;
- In section 3, we present what Endeavour Energy has proposed for cyber security, as the basis for our assessment; and
- In section 4, we describe our assessment of Endeavour Energy's proposed cyber security allowance, our findings on the prudency and efficiency of that allowance and the implications of those findings for the expenditure allowance that Endeavour Energy has proposed.

1.4.2 Information sources

21. We have examined relevant documents that Endeavour Energy has published and/or provided to AER in support of the areas of focus and projects that the AER has designated for review. This included further information at a virtual meeting 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 to us prior to 1st July 2023 and any information provided subsequent to this time may not have been taken into account.

1.4.3 Presentation of expenditure amounts

23. Expenditure is presented in this report in $2024 real terms, to be consistent with Endeavor Energy's RP, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.

24. While we have sought 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 RELEVANT CONTEXT TO OUR ASSESSMENT

We have conducted our review in the context of increasing cyber security threats and a typically increasing threat surface, taking account of relevant regulatory compliance obligations and industry frameworks for assessing cyber risk criticality and risk mitigation maturity.

2.1 Cyber security threat in Australia

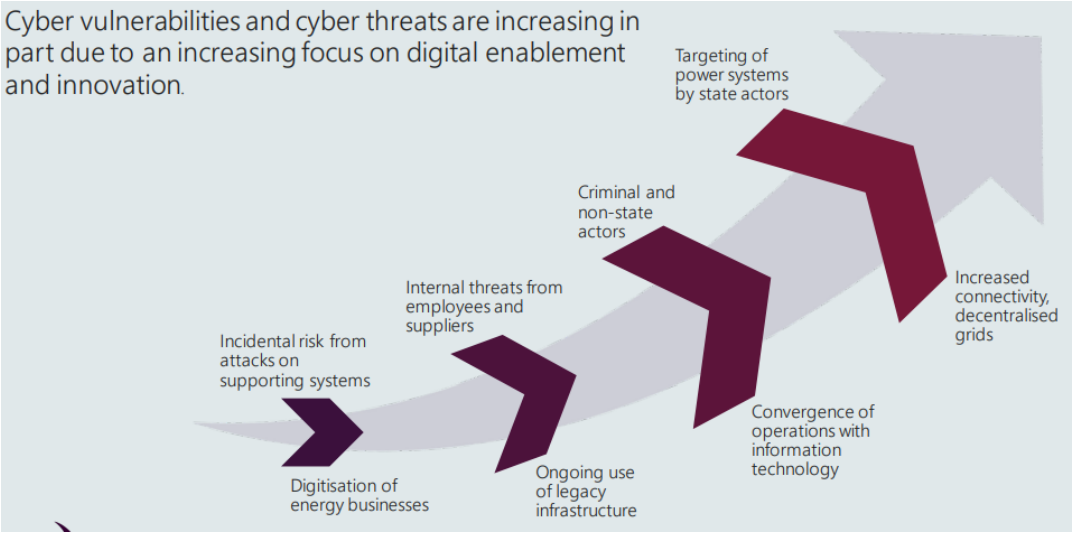
25. The Australian Cyber Security Centre ('ACSC') monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2021-22) it states that: *The ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year.* In the same report it identifies the following cyber security trends:

- *Cyberspace has become a battleground.*
- *Australia's prosperity is attractive to cybercriminals.*
- *Ransomware remains the most destructive cybercrime.*
- *Worldwide, critical infrastructure networks are increasingly targeted. Both state actors and cybercriminals view critical infrastructure as an attractive target. The continued targeting of Australia's critical infrastructure is of concern as successful attacks could put access to essential services at risk. Potential disruptions to Australian essential services in 2021–22 were averted by effective cyber defences, including network segregation and effective, collaborative incident response.*
- *The rapid exploitation of critical public vulnerabilities became the norm…The majority of significant incidents ACSC responded to in 2021–22 were due to inadequate patching.*

26. The Electricity, Gas, Water and Waste services sectors accounted for 3% of cyber security incidents in 2021-22. Among other things the ACSC promotes the Essential Eight cyber security measures.

27. At its 2022 AESCSF education workshop with the Department of Industry, Science, Energy and Resources, AEMO discussed cyber threat actors, motivations, and case studies and included the following figure in its presentation.

Figure 2.1: The cyber security problem



Source: AEMO, 2022 Australian Energy Sector Cyber Security Framework Education Workshop, slide 5

28. This figure highlights the twin issues of increasing cyber-attack threat landscape and the increasing vulnerability of electricity utility assets due to the increasing 'attack surface' presented due to increased digitalisation and interconnectivity.

2.2 Critical infrastructure - changes to regulation

2.2.1 Amendments to the SOCI Act

29. The Security of Critical Infrastructure Act 2018 ('SOCI Act') places obligations on specific entities in the electricity and other industries.

30. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) has recently amended the SOCI Act to strengthen the security and resilience of critical infrastructure by expanding the sectors and asset classes the SOCI Act applies to, and to introduce new obligations.

31. The amendments were made because '*Australia is facing increasing cyber security threats to essential services, businesses and all levels of government.* [1] Electricity assets can be classed as critical infrastructure within the framework under the Act. The new 'Positive Security Obligations' that apply to certain sets of critical infrastructure assets are:

- Register of Critical Infrastructure Assets: which requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide to Government ownership, operational, interest and control information; and
- Mandatory Cyber Incident Reporting: Responsible entities for critical infrastructure assets will be required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal.

32. On 2 April 2022, additional amendments to the SOCI Act introduced the following:

- A new obligation for responsible entities to create and maintain a critical infrastructure risk management program ('CIRMP') with the obligation commencing on 17 February 2023;[2] and

1 Department of Home Affairs, Cyber and Infrastructure Security Centre website

2 CISC Factsheet – Risk Management Program

- A new framework for enhanced cyber security obligations (ECSO) required for operators of systems of national significance (SoNS), Australia's most important critical infrastructure assets.[3]

33. The CIRMP is a written program which requires a responsible entity for a critical infrastructure asset to (i) to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, and so far as it is reasonably practicable to do so, (ii) minimise or eliminate any material risk of such a hazard occurring, and (iii) mitigate the relevant impact of such a hazard on the asset.[4]

34. The ECSO will vary between each SoNS, depending on the specific role and function of that asset, with the obligations including (i) developing cyber security incident response plans to prepare for a cyber security incident, (ii) undertaking cyber security exercises to build cyber preparedness, (iii) undertaking vulnerability assessments to identify vulnerabilities for remediation, and/or (iv) providing system information to develop and maintain a near real-time threat picture.[5]

2.2.2 CIRMP - AESCSF Security Profile 1 and Essential Eight Maturity Model

35. 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.[6] 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.[7]

36. 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 NSPs must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.

37. 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.

2.2.3 Privacy Act amendments 2022[8]

38. The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 ('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.

39. 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 $2.22m.

---

3 CISC Factsheet – Systems of National Significance and Enhanced Cyber Security Obligations

4 Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 – explanatory statement

5 Department of Home Affairs, Cyber and Infrastructure Security Centre website

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

7 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)

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

40. 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.* [9]

2.2.4 Distributor's Licence under the Electricity Supply Act 1995 (NSW) – Licence Conditions Variations[10]

41. Critical Infrastructure Licence Conditions 9 (Substantial presence in Australia), 10 (Data Security), and 11 (Compliance) of the Licence and are of relevance to DNSPs in NSW. Within these Conditions there are multiple requirements. Among other things, Condition 11 requires the Licence Holder to report to the Tribunal by 30 September each year detailing how it has complied with conditions 9 and 10 over the preceding financial year.

2.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

2.3.1 AESCSF V1

42. 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 voluntary but has been adopted by NSPs.[11] The AESCSF is divided into 11 domains, ten C2M2[12] 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.[13] AESCSF Version 1 (V1) encompasses the 2018 and subsequent iterations up to and including the 2022 revision.

43. 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.

44. 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 TNSPs rated as High criticality and with DNSP criticality rating ranging between the High and Medium bands.

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

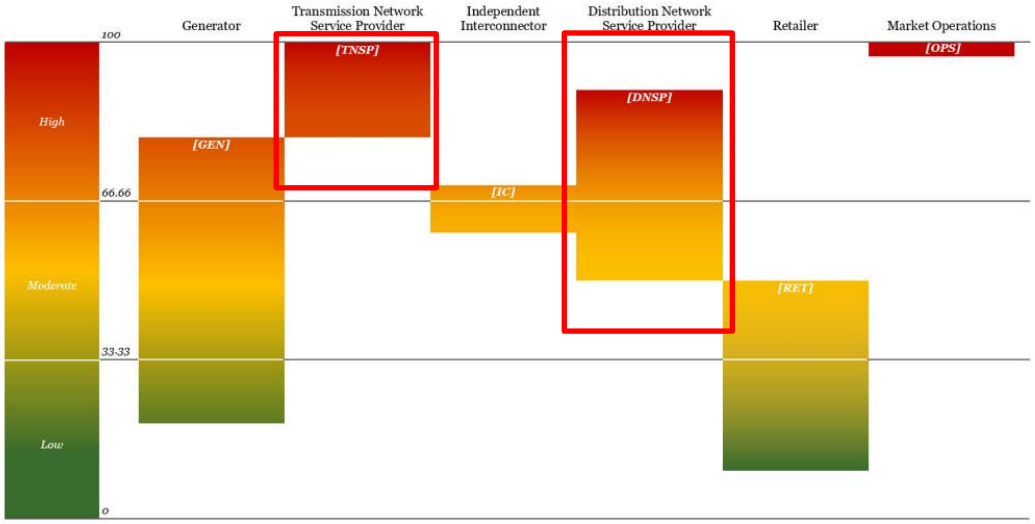
10 The Minister for Resources and Energy issues the DNSP licences. IPART administers compliance with the licence conditions on behalf of the Minister. Licence conditions for Ausgrid are available from IPART's website

11 AEMO, AESCSF Framework and Resources, AEMO website

12 United States Department of Energy Cyber Security Capability Maturity Model

13 AEMO AESCSF Framework Overview – 2022 Program, page 1

Figure 2.2: AESCSF E-CAT criticality bands for electricity sector – TNSPs and DNSPs highlighted



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

45. The table in the figure below '*indicates which* SP *an organisation in the electricity sub-sector should achieve based on their criticality (as determined by the E-CAT)*.'[14] This may be construed as an obligation, however AEMO also states 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.*[15]

Figure 2.3: Relationship between SPs, participant criticality, practices/anti-patterns and MILs – per AESCSF V1

Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	Mil-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP-2)

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

46. To help organisations define roadmaps to improved cyber security maturity, the ACSC included guidance on 'Priority Practices' within each SP. The Priority Practices are recommended for completion first as part of any uplift program. There are 20 priority practices across the 11 domains within SP-1, 5 across 5 domains in SP-2 and one in the ACM[16] domain in SP-3.[17]

2.3.2 AESCSF Version 2 (V2)

47. 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

14 AEMO AESCSF Framework Overview – 2022 Program, page 9

15 AEMO AESCSF Framework Overview – 2022 Program, page 3

16 Asset, Change and Configuration Management

17 AEMO AESCSF Framework Overview – 2022 Program, pages 9, 20

security requirements for the energy sector in line with escalating and evolving cyber threats.

> *'AEMO has worked in partnership with DCCEEW and the Department of Home Affairs Critical Infrastructure Centre (CISC) on the 2023 Program to support energy organisations' continued cyber maturity journey and to support energy organisation's Risk Management Plan (RMP) regulatory obligations under the SoCI Act.'*[18]

48. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting RMP minimum obligations), and a transition plan to 'sunset' AESCSF V1.

49. The release of AESCSF V2 was scheduled for May-June 2023, but at the date of writing this report, no further information about the V2 is available on the AEMO website.

2.4 AER Guidelines for non-network ICT assessment

2.4.1 Assessment of non-network ICT capex

50. The scope of our assessment includes cyber security capex and opex and is categorised as non-network ICT.

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

52. 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:[19]

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

53. 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.*[7] *For such investments, we consider that they should be justified on the basis of the 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.'*

Complying with new / altered regulatory obligations / requirements

54. 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.'*

New or expanded ICT capability, functions and services

55. 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.*

56. *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*

---

18 AEMO website, AESCSF Program

19 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

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.

57. *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*.'

2.4.2 Assessment of opex step changes

58. 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:[20]

- 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.

2.5 Implications for our assessment

Increasing threat landscape and attack surface mean cyber risk is increasing

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

60. In our assessment we have sought to understand how Endeavour Energy 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 four aspects of the (amended) SOCI Act and from consideration of certain amendments to the Privacy Act

61. 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; and
- CIRMP, which requires completion of all the practices (and absence of anti-patterns) required to achieve SP-1 (per AESCSF V1) by mid-2024, noting that SP-1 is the least onerous of the security profiles under the AESCSF.

62. If NSPs are classified as a SoNS, then ESCOs apply and which are applied on a case-by-case basis to the NSPs.

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

[20] AER, Expenditure Forecast Assessment Guideline for Electricity Distribution, p11

64. We have assessed how Endeavour Energy 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.

65. We have also considered whether Endeavour Energy has identified any other relevant obligations.

Licence Conditions Variations to a Distributor's Licence under the Electricity Supply Act 1995 (NSW) do not represent new obligations

66. The Instrument of Variation to the Distributor's Licence has been available since 2019. We consider that Endeavour Energy should by now have responded to the conditions. We therefore consider that the opex implications of the Licence variations will be a part of the efficient base year and there are unlikely to be new non-recurrent capex or recurrent opex/opex step change arising from the variations.

AESCSF V1 was available for the preparation of Endeavour Energy's RP but the intent of V2 has already been promulgated

67. AESCSF V1 was the current version when Endeavour Energy prepared its RP and therefore the extent to which it has referenced this Program and, possibly, the Priority Practices, in developing its cyber security forecast expenditure for the next RCP is relevant.

68. However, it is also relevant to consider the extent to which Endeavour Energy has incorporated other frameworks, if any, into its proposed expenditure.

69. Whilst AESCSF V2 has not been publicly released at the time of writing this report, we assume that because V2 was '…*developed in consultation with industry, governments and specialist agencies*…'[21] that Endeavour Energy was broadly aware of the likely increase in the hurdles (number of practices) to achieve each of the three MILs and three SPs compared to V1. Again, it is relevant to take into consideration Endeavour Energy's incorporation of future regulatory obligations where there is a reasonable evidenced understanding of what they will be, noting that it has the opportunity for applying to the AER for a pass through if new obligations occur after approval of its RP and which could not reasonably have been anticipated.

70. It is reasonable also to consider Endeavour Energy's E-CAT score (if available) and its target SP level at the end of the current RCP and at the end of the next RCP, the initiatives it proposes to achieve them and by when, and the estimated costs of each.

[21] AEMO website, AESCSF Program

3 ENDEAVOUR ENERGY'S PROPOSED ICT CYBER SECURITY EXPENDITURE

Endeavour Energy has proposed a cyber security-related capex allowance of $16.3m. It did not propose an opex step change.

Endeavour Energy has recently advised the AER of an amended and considerably higher proposed capex allowance and also has introduced a proposed opex step change; however this was provided after our assessment of its regulatory proposal allowance.

3.1 Overview and summary of proposed expenditure

3.1.1 What Endeavour Energy proposed in its RP

71. Endeavour Energy has proposed cyber security-related ICT capex of $16.3m. In its RP, Endeavour Energy has not proposed a cyber-security related opex step change, though it records that it will incur $4.4m opex over the period.

Table 3.1: Endeavor Energy proposed ICT cyber security related expenditures - $million, real FY2024

Description	2025	2026	2027	2028	2029	Total
Non-recurrent ICT-compliance capex (cyber security)	3.3	3.3	3.3	3.3	3.2	**16.3**

Source: Endeavour Energy, Investment Brief 3, Table 7

3.1.2 Endeavour Energy's replacement business case

72. In its RP, Endeavour Energy stated that it would advise an opex step change amount at some later time:[22]

> *'…there remains a degree of uncertainty of the costs and timing associated with SOCI compliance. On this basis, we do not consider the step change is reasonably quantifiable at this stage of the determination process noting work is ongoing to clarify and confirm the cost of compliance. We will continue to consult on our position in advance of our Revised Proposal.'*

73. In response to an Information Request, Endeavour Energy provided a Cyber Security 'Business Case' in mid-July, and which it appears Endeavour Energy considers as replacing its Regulatory Proposal in regard to cyber security expenditure:[23]

> *'As foreshadowed in our 2024-29 Regulatory Proposal, we had yet to determine the costs of compliance with the SOCI Act at the time of submitting the Regulatory Proposal given the complex analysis required to support a robust investment in cyber security. This business case represents the additional analysis we have undertaken to support our cyber security investment and to ensure compliance with the SOCI Act.'*

74. The options considered in the Business Case appear to be similar to what we inferred from the information Endeavour Energy provided in and with its RP, however the proposed total

22 Endeavour Energy-0_01 Regulatory Proposal – January 2023-Public, page 238

23 Endeavour Energy - IR015 - SOCI Cyber Appendix 2 CFI - Confidential – 20230712, page 7

cost for its preferred option is over three times higher, at $68.03m (real FY23) comprising $33.00m capex, $18.06m 'project' opex and $16.97m recurrent opex.

75. The Business Case was received well after our cut-off date for considering new, significant material to assist with our assessment of Endeavour Energy's RP and is in substance a different proposal. For the avoidance of doubt, we have assessed in this report what Endeavour Energy proposed in its RP.

3.2 Summary of the basis for Endeavour Energy's proposed expenditure

3.2.1 Documents supporting proposed cyber security program

76. Endeavour Energy initially provided two core documents to support its cyber security strategy, initiatives and investment:

- Its ICT Asset Strategy 2024-2029 (ICT Strategy); and
- Its ICT Strategy 'Investment Brief 3 – Providing a resilient network for the community adapting to changing climate and external hazards' (IB3).

77. As the IB3 theme indicates, the document covers a range of matters, including climate resilience (extreme weather events) as well as cyber security threats and cyber security compliance obligations. Similarly, the ICT Strategy itself covers multiple topics, including cyber security.

3.2.2 Problem definition and risk assessment

78. In its ICT Strategy the increase in cyber security risk is recognised, as is the need to respond to this risk: *Increased focus on security will be required as cyber-attacks become more frequent and sophisticated.*[24]

79. Two drivers of investment in cyber security are identified in Endeavour Energy's IB3: '*Withstand*' and '*Respond and Recover*', both of which are said to derive a benefit of '*meeting mandatory requirements for cyber security and SOCI.*'

80. Endeavour Energy's RP also provides an analysis of the changes to the Security of Critical Infrastructure Act (SOCI Act), including the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth) (SLACIP Act).

3.2.3 Endeavour Energy's cyber security strategy and objectives

81. Endeavour Energy's ICT Strategy includes the following '*outcome description*' for the next RCP, which we infer to encapsulate its strategy:

> *'Protect ICT infrastructure and data by being responsive, predictive and proactive to security risks in order to provide trust to the customer, Board and Security Industry standards."*[25]

82. Endeavour Energy outlines '*strategic responses*' to the threat of increasing cyber-attack in its IB3:[26]

- **Strategic Response 4**, which is '*Enhancing cyber resiliency through the uplift of cybersecurity platforms and enablers to provide insights on the security status of the technology environment and protect against evolving threats.*' The objectives and outcomes of this strategic response are stated as:

[24] Endeavour Energy – ICT Asset Strategy 2024-2029, page 25

[25] Endeavour Energy ICT Asset Strategy, page 11

[26] Endeavour Energy Investment Business Case 3, pages 18, 19

  - Uplifted cybersecurity platforms and enablers
  - Enhanced cybersecurity insights and exposures, and
  - Enable cyber security culture and organisational resilience;
- **Strategic Response 5**, which is '*Maintaining network infrastructure and uplifting future network capability to avoid service disruption and maintain safe and resilient supply of networks.* Relevant objectives and outcomes of this strategic response are stated as:
  - Enhanced security to applications, data and services, and
  - Integrated network to support connectivity capabilities; and
- **Strategic response 6**, which is '*Enhancing corporate and business system platforms to uplift asset maintenance, resource management and risk and compliance.'* The relevant objectives and outcomes of this strategic response are stated as:
  - Integrated IDM/IAS, and
  - Enhanced governance risk and compliance.

3.2.4 Endeavour Energy's cyber security current state

83. The ICT Strategy reports that a Security Implementation Plan (SIP) was implemented in the current RCP and '*allowed Endeavour Energy to continue to operate and meet the Distributor's Critical Infrastructure Licence Conditions 9 and 10,*[27] among other things.[28]

84. There is no specific information about Endeavour Energy's current cyber security maturity level or cyber security program of work in the ICT Strategy or IB3. However, in response to an Information Request, Endeavour Energy provided a report on an AESCSF Gap Analysis[29] from March 2022 that records that:

- Of the 77 'controls' reviewed for SP-1, [redacted] of them were fully implemented [redacted] or largely implemented [redacted]; and
- Of the 101 'controls' reviewed for SP-2, [redacted] were Fully implemented [redacted] or largely implemented [redacted].

3.2.5 Options considered by Endeavour Energy for managing cyber security obligations and risks

85. Endeavour Energy considers three options in the IB3:[30]

- **Option 1 -** Ensure regulatory changes and improved response to vulnerable customers – the focus is on ensuring '*cyber, business continuity and network resilience and an active response to regulatory changes and to vulnerable customers';*
- **Option 2:** Ensure regulatory changes, improved response and recovery to all customers, and improved anticipation of weather events and energy market transition – the focus is to *forecast weather events and energy market transition, as well as ensure network and business continuity/reliability…';* and
- **Option 3:** Ensure regulatory changes, improved anticipation, response and recovery, and improved learning and adaptation capabilities – the focus is on '*developing insights and understanding to improve processes through greater information sharing from implementation of new innovations and data sources. This option specifically focuses on long-term view of the network.'*

27 Endeavour Energy ICT Asset Strategy, page 13

28 Endeavour Energy ICT Asset Strategy, page 17

29 Endeavour Energy - IR015 - Secolve EE Gap Analysis - Confidential - 20230504

30 Endeavour Energy Investment Brief 3, pages 20-22

86. Endeavour Energy has proposed Option 3 in which the cyber security component cost is $20.70m, comprising $16.3m capex and $4.4m opex (including a capex contingency allowance).

87. Endeavour Energy has not submitted an opex step change in its RP, however we note comments in its RP regarding its intention to revise its cost estimate (among other things) in its RRP and Endeavour similarly stated at our onsite review meeting that it intended to propose an opex step change but had not yet done so at that time.

4 OUR ASSESSMENT

While Endeavour Energy's cyber security-related objectives are not clearly stated, from the information that it provided we consider its cyber risk target is appropriate and that its proposed program is reasonable, given its level of criticality. Except for a project contingency allowance, we consider that Endeavour Energy's forecast capex allowance is reasonable.

4.1 Observations on Endeavour Energy's current state

Endeavour Energy's current cyber security program is unclear

88. It is not clear from the information provided what Endeavour Energy has or is intending to spend on what initiatives in the current RCP.

89. Endeavour Energy's March 2022 AESCSF cyber security assessment concluded that [redacted] of SP-1 practices had been fully or largely implemented and [redacted] of SP-2 practices were fully or largely implemented. This suggests that at least an SP-1 level should be achieved by the end of the current RCP.

90. In response to an Information Request, Endeavour Energy provided the figure below and advised that it needs to implement only [redacted] more practices (out of the 200 practices and anti-patterns required) to achieve SP-2.

91. In the absence of information to the contrary, we assume that Endeavour Energy will have built the necessary practices to ensure it continues to comply with its cyber security related IPART Licence conditions. This would in turn mean that the efficient costs for compliance are already included in its Base Year efficient opex.

4.2 Endeavour Energy's risk analysis

92. Endeavour Energy has provided a qualitative risk assessment in its IB3 document. In this section we assess whether the risk analysis is sufficiently compelling to support the proposed cyber security investment in the next RCP.

Endeavour Energy's risk assessment is high level and challenging to interpret

93. Endeavour Energy's IB3 includes a risk mitigation analysis relevant to cyber security in addressing corporate risks R1.2 and R1.3:

> *'R1.2 Network - Maintaining network reliability and capacity, health, currency and sustainability of assets to ensure timely provision of infrastructure or solutions to service customers whilst considering future energy consumption. This includes building and maintaining a set of security capabilities that meet critical infrastructure obligations and minimise the threats arising from malicious attacks and/or risks to the availability and integrity of network or systems which support critical business functions.'* [31]
>
> *R1.3 Customer - Maintaining a customer-centred and performance-driven culture to act to resolve customer complaints promptly and fairly, analyse trends to drive continuous improvement.'*[32]

94. In relation to Risk R1.2, in Table 16 of the IB3 document, Option 1 is said to make a Medium contribution to risk mitigation, Option 2 is said to make a High contribution to risk mitigation, and Option 3 will make a Very high contribution to risk mitigation.

95. In respect to Risk R1.3, in Table 16 of the IB3 document, Option 1 is said to make a Low contribution to risk mitigation, Option 2 said to make a Medium contribution to risk mitigation and Option 3 will make a High contribution to risk mitigation.

96. In its IB3 document, the reader is advised that '*Table 16 assesses the contributions of the three options to mitigation of the five corporate risks associated with this investment brief*', however there is no qualitative assessment to support the risk analysis. In addition to the lack of precision of the wording of risks R1.2 and R1.3 regarding cyber security, interpretation of the claimed risk mitigation from each option with respect to cyber security is challenging and regardless is neither particularly insightful nor compelling.

97. In relation to the increased risk from an increasing 'attack surface' presented by the 'digitalisation of network businesses' we could find only one reference in Endeavour Energy's core documents, namely the recognition of the need to '*reduce the cyber-attack surface*'.[33] This is listed as an objective of the '*enable*' phase of its IB3.

4.3 Endeavour Energy's cyber-related objectives

It is unclear from Endeavour Energy's documentation whether it is seeking to maintain or to improve its cyber risk over the duration of the next RCP

98. Absent clear statements in Endeavour Energy's documentation, we have sought to infer its cyber risk mitigation objective. A possible interpretation of Endeavour Energy's risk assessment is that it is aiming to maintain its cyber security risk level in the face of rising cyber security threats and its increasing attack surface. To maintain the risk level (and comply), cyber security capabilities do need to increase. However, this interpretation is somewhat undermined by Endeavour Energy's statement that *'[n]o projects under this investment brief are categorised as maintaining existing capabilities in the following regulatory period.* [34].

99. Endeavour Energy attributes all the non-recurrent costs to '*compliance*'. However this interpretation could only be supported if Endeavour Energy is taking a broad interpretation of the term 'compliance' with respect to the AER's guideline for non-recurrent capex, intending it to address both minimum legislative compliance obligations and also alignment to AEMO's AESCSF criticality level (and assuming SP2 as a target).

31 Endeavour Energy, Investment Brief 3, page 44

32 Endeavour Energy, Investment Brief 3, page 44

33 Endeavour Energy, Investment Brief 3, page 26

34 Endeavour Energy, Investment Brief 3, page 35

Endeavour Energy identifies its cyber security-related compliance obligations

100. Endeavour Energy identifies that regulatory compliance obligations are 'growing' in response to the increasing cyber security threat to the Australian government, its agencies, and Australian businesses, including changes to:

- The SOCI Act (including the SLACI Act, the SLACIP Act and the CIRMP Rules), and
- The NSW electricity distributor licence conditions.

101. Changes to the Privacy Act do not appear to be recognised in Endeavour Energy's documentation provided to us.

Endeavour Energy's objectives include acquittal of its legislative compliance obligations

102. Endeavour Energy is consistent in its core documents regarding the need for its cyber security investment to acquit and sustain its compliance obligations. As we discuss in section 4.1, Endeavour Energy has not indicated that it requires any incremental expenditure in the next RCP to address its IPART Licence cyber security obligations.

Endeavour Energy is targeting SP-2 in the next RCP which is a reasonable target

103. Section 3.2 describes Endeavour Energy's strategic objectives as a combination of '*outcome descriptions*' and '*strategic responses*.' The documents these were derived from are not specific regarding alignment with the AESCSF, however in response to an Information Request, Endeavour Energy advised that '*The Endeavour Energy Board approved the Cyber Security Strategy and SP2 maturity level on 30 March 2023.*'[35]

104. In the absence of evidence from Endeavour Energy that its E-CAT criticality rating is '*High*' we consider that its likely network criticality is '*moderate'.* If this is the case, then based on the AESCSF guideline, SP-2 is likely to be a prudent target for the next RCP for Endeavour Energy, noting that in March 2022 it was assessed as being almost at SP-1 and in 2023 it was only [redacted] practices short of achieving SP-2.

4.4 Endeavour Energy's options analysis

4.4.1 Overview of options

105. Endeavour Energy presents three options in its IB3 document. Option 2 builds on Option 1 and Option 3 builds on Option 2.

106. Endeavour Energy did not present its analysis of a 'Do Nothing' / 'Business as Usual' option.[36] In our view, inclusion of a BAU option is consistent with good industry practice, particularly as it can be positioned as the counterfactual for economic analysis of the options.

Endeavour Energy's summary of its options analysis provides no meaningful comparative analysis of its cyber security investment options

107. Endeavour Energy presents both a qualitative and quantitative options analysis summary in its IB3 document. In response to an Information Request, Endeavour Energy has also provided a cost-benefit analysis spreadsheet which is the source document for the claimed quantitative benefits. We assess the construct and the outcomes of both analysis tools in this section.

108. We consider there may be some value in the selection criteria, the weighting, and the scoring system described in section 3.2 of the IB3 document at the '*whole of IB3*' program level. However, Endeavour Energy's bundling of cyber security 'resilience' with many other

[35] Endeavour Energy – IR015 – response – Public, page 11

[36] However we note in its response to an information request, a BAU cost of $25.52m is identified. No context is provided for this that we are aware of – refer to Endeavour Energy – IR015 – Cost build up SP2 – Confidential – 20230504

objectives, strategies, and initiatives in IB3 means that there is no discernible contribution to the comparative options analysis from a cyber security perspective in Table 1 of the IB3 document.

4.4.2 Option 1 – Ensure regulatory changes and improved response to vulnerable customers

Option 1 includes six initiatives to address cyber security resilience gaps

109. Endeavour Energy describes this option as '*reactive investment*' and further advises that Option 1 addresses two of its four investment drivers, both of which lead to benefits of '*Meeting mandatory requirements for cybersecurity and SOCI*':[37]

- Withstand – to maintain network resilience through capabilities which predict and detect security threats for early intervention, as well as effective response; and
- Respond and recover – to maintain its operations to provide vulnerable customers with consistent service.

110. The Option 1 initiatives related to cyber security are:[38]

- Strengthening governance and standards;
- Enable smooth adoption of technologies and solutions;
- Building resilience to the ever-changing cyber threat environment;
- Securing digital identities and data;
- Enable a cyber safe workforce of the future; and
- Working with secure suppliers and partners.

The lack of relevant information makes assessment of the merits of Option 1 challenging

111. As there is no mapping of these initiatives by Endeavour Energy to (i) the AESCSF domains, (ii) achievement of the complete suite of SP-2 practices and anti-patterns (i.e. addressing the [redacted] practices gap), or (iii) its compliance obligations, we cannot be confident that Option 1 is or is not a prudent option.

Endeavour Energy's assessment of this option is summarised in two paragraphs:

> *'[it] has a lack of initiatives supporting the two key strategic external drivers which support the future network needs…and insufficiently meet the needs and expectations of customers in how Endeavour Energy prioritises investments.'*[39]

> *'it] does not permit proactive investment to anticipate and respond to external hazards and events, instead focusing on reactive responses to cyber and data threats. Additionally, the lower alignment with the suite of customer priorities demonstrates it does not sufficiently meet the expectations of customers in the forthcoming regulatory period.'* [40]

However, as Option 1 includes initiatives which are far broader than addressing cyber security gaps, Endeavour Energy's own assessment is not directly relevant to cyber security options analysis. Further, the assessment is essentially a tautological redefinition of the option itself, given that it is labelled as '*reactive investment*' and asserts without evidence that it '*insufficiently meets ...needs and expectations.'*

---

37 According to Endeavor Energy's Investment Logic Map , Figure 2 in its Investment Brief 3 document, page 8

38 Endeavour Energy, Investment Brief 3, Table 13 first strategic response

39 Endeavour Energy, Investment Brief 3, page 24

40 Endeavour Energy, Investment Brief 3, page 24

4.4.3 Option 2 - Ensure regulatory changes, improved response and recovery to all customers, and improved anticipation of weather events and energy market transition [41]

Option 2 does not appear to include any additional cyber security initiatives

112. Endeavour Energy refers to Option 2 as '*predictive investment*'. The focus of Option 2 is to *forecast weather events and energy market transition*, as well as *ensure network and business continuity/reliability*. This option specifically focuses on short term anticipation of network issues.

113. There are no discernible additional cyber security initiatives in Options 2's scope of work. We therefore do not consider it from this point forward because it is equivalent to Option 1 in terms of scope, cost, timing, and benefits for cyber security resilience.

4.4.4 Option 3: Ensure regulatory changes, improved anticipation, response and recovery, and improved learning and adaptation capabilities (Endeavour Energy's preferred option)

Option 3 similarly does not appear to include any additional cyber security initiatives

114. Endeavour Energy refers to this option as '*pre-emptive investment*', which '*specifically focuses on long-term view of the network*.' In addition to the drivers addressed under Option 1, Option 3 addresses:[42]

- Learn & Adapt - Endeavour Energy '…*must ensure it maintains capabilities in data, analytics & insights and automation to respond to and learn from disruptive events…*'
- Anticipate (Long Term) - Endeavour Energy needs to ensure it has the capability to forecast the future.

115. As far as we can discern from the IB3 description and its CBA model there are only six cyber security initiatives (also referred to as projects[43]) and Option 3 does not add to them. We note reference in Table 13 of IB3 to '*application of zero trust network transformation*' but we assume this is within the scope of one of the six initiatives.

The lack of relevant information from Endeavour Energy makes assessment of the merits of Option 3 challenging

116. Endeavour Energy's own assessment of Option 3 relative to Option 1 and Option 2 is that it '…*more strongly supports the external investment drivers and customer priorities identified as important to delivering the outcomes in this Investment Brief. Furthermore, the level of benefits achieved across the firm from investment under this option offsets the higher capital costs required to provide a resilient network.*'[44]

117. Again, because Option 3 comprises a scope of work far wider than the initiatives to maintain cyber security risk and achieve SP-2, and because of the limitations of Endeavour Energy's comparative analysis, it is difficult to conclude that any more than the Option 1 initiatives are warranted.

118. Whilst Option 3 is Endeavour Energy's proposed option, we consider it to be materially the same as Option 1 from a cyber security perspective. We have therefore focussed on the initiatives that are included in Option 1 for the remainder of our assessment.

---

41 Endeavour Energy, Investment Brief 3, page 20

42 Endeavour Energy, Investment Brief 3, page 21

43 Specifically, projects 164-169 which are designations applied in the CBA model and grouped as Program 16

44 Endeavour Energy, Investment Brief 3, page 24

4.5 Endeavour Energy's cost forecasting methodology

Endeavour Energy's cost forecasting methodology appears to be appropriate with one exception - the inclusion of project contingency

119. Endeavour Energy has described its cost forecasting methodology (via its '*key assumptions*') in the IB3 document. With the exception of a capex contingency provision of 19%, we consider that Endeavour Energy's cost forecasting methodology follows common practice. Inclusion of project-level contingency amounts is not warranted in an RP submission for an aggregate portfolio-level expenditure allowance.

120. We summarise other aspects of Endeavour Energy's forecasting methodology as follows:[45]

- The estimate is a bottom-up construct from the cost for individual scope elements;
- Scaling is used based on scope and complexity, combined with historical delivery experience and knowledge of potential purchases;
- The cost differentiates between its planned resourcing mix (i.e. hybrid insource/outsource model);
- Infrastructure maintenance is a recurrent percentage of 5.8% of project costs;
- Forecast labour costs are based on typical unit rates / day rates; and
- It has incorporated external advice to both help define the scope and refine the cost estimates.

Endeavour Energy commissioned external review of its cyber security cost estimate[46]

121. Endeavour Energy commissioned a market comparison (aka 'benchmarking') of its proposed cyber security projects. The consultant's report is dated September 2022. It provides benchmarking information and observations of cost estimations and sizing of the projects undertaken based on a target of SP-2.

122. Confusingly, the major projects which were the subject of the external analysis do not align fully with the six projects referred to by Endeavour Energy in its IB3 document and its CBA model.[47] This is not explained.

123. In summary, from the benchmarking study we observe that:

- Most of the project costs are above the mid-point of the market comparison range; and
- With respect to the 'allocated budget', which is in aggregate, $22.34m ($13.4m capex, $8.9m opex):
  - whilst it is not stated explicitly, we assume the cost base is real $FY24 and that contingency is included;
  - this is more than the $20.7m totex proposed in the IB3 document but not excessively so – we assume that the RP expenditure of $20.7m was derived taking into account the external review;
  - it is less than the cost of $25.5m ($15.15m capex and $10.39m opex) identified in a response to an Information Request[48]
  - it is less than the $25.5m without program overheads and contingency ($17.85m capex and $7.7m opex) in the CBA model provided.

[45] Endeavour Energy, Investment Brief 3, page 34

[46] Endeavour Energy - IR015 - Cyber Strategy Deloitte Risk Advisory Review Report - Confidential - 20230504

[47] For example, there is a 'Cyber Defence Centre' initiative in the 'major projects list which is estimated by Endeavour Energy to cost $5.2m and which is not one of the six 'IB3' projects

[48] Endeavour Energy – IR015 – Cost build up SP2 – Confidential - 20230504

124. We are not sure of the reconciliation between these sources, but we have undertaken our assessment on the basis of the amount submitted in the IB3 document, which is $20.7m totex (including overheads and a capex contingency allowance).

The capex:opex ratio for ICT cyber security projects is unusually weighted heavily to capex

125. In our experience, contemporary ICT expenditure forecasts exhibit a heavy weighting to opex due to accounting requirements and the move to cloud-based products (and the associated subscription services and/or licence fees). The capex-opex split is typically 20% to 30% non-recurrent capex with the balance as opex (a mixture of recurrent and non-recurrent).

126. Endeavour Energy's proposed expenditure forecast is heavily weighted to capex, which is not satisfactorily explained.

4.6 Other aspects

4.6.1 Economic justification

The CBA analyses do not provide a usable assessment of the economics of the proposed projects; however economic justification is not required if Endeavour's program is to maintain its cyber security risk level

127. We find that there are common issues with Endeavour Energy's cost-benefit analyses[49] which we discuss below. To the extent that Endeavour Energy's proposed expenditure needed to be supported by economic analysis, the issues individually and collectively result in what we consider to be unreliable outputs and would not provide adequate justification of the non-recurrent new-compliance capex sought by Endeavour Energy.

128. However, as discussed above, given that we interpret Endeavour Energy's intent as maintaining its cyber security risk level and to comply with its legislative and other obligations, a positive NPV is not a necessary feature in the prudency and efficiency test. Further since Option 1, 2 and 3 are essentially the same from a cyber security perspective, there is no value required from the CBA model for comparative analysis.

Endeavour Energy's representation of NPVs and Benefit Cost Ratios is flawed

129. Endeavour Energy's CBA models include what are described as Net Present Values (NPVs) and Benefit Cost ratios (BCRs). These would normally provide measures of the economic net benefit of a project, based on some form of discounted cashflow analysis, taking account of the time value of money through application of a Weighted Average Cost of Capital (WACC).

130. We find that neither NPVs nor BCRs in the Endeavour Energy's economic models incorporate any concept of discounted cashflow analysis or application of the time value of money. There are therefore no usable metrics in Endeavour Energy's CBA models that would demonstrate the economic value of the projects that it has proposed.

Most types of benefits are intuitively logical, though little evidence is provided to support the values

131. In Endeavour Energy's CBA model for IB3, the cyber security projects are linked to the following benefit streams, and which are intuitively logical:

- Avoided loss from cybercrime;
- Productivity loss; and
- Avoided system failure costs.

[49] Endeavour Energy, 03. Investment Brief 3 v1.2 CBA

132. However, a '*reduction in cancelled maintenance works*' benefit stream is also included in the analysis and does not appear to be reasonably linked to the six cyber security projects.

133. Endeavour Energy advises that its methodology for calculating and validating the quantitative benefits involved thorough internal consultation and '*extensive research and communication with external stakeholders*'. However, it is unclear what input external stakeholders actually had, or reasonably could have had, to quantifying the types of benefits listed.

Simplifying assumption for apportioning benefits masks 'true' benefits of each proposed project

134. In the CBA model we find that Endeavour Energy has typically calculated a particular benefit for a cluster of projects as an aggregate amount. It has then apportioned this aggregate amount between the projects in the cluster for which it considers the 'type' of benefit to be relevant.

135. Where such projects are interdependent, this could be a valid approach. However, Endeavour Energy provides no indication of the dependencies between the 'clustered' projects and for the most part it appears that the projects are independent and therefore each would warrant separate assessment of its benefits. There is nothing in Endeavour Energy's calculation to suggest that the aggregate benefit would only occur if it was to undertake all the projects to which that benefit has been apportioned. And we find that in practice, for the six cyber security projects, benefits are apportioned between projects based on their cost. This masks any valid assessment of benefits for a particular project and therefore undermines the ability to assess the economics of any specific project.

136. This issue makes it challenging for the reviewer and, we suspect, Endeavour Energy itself, to understand which of the six projects are likely to add true value.

There is some potential for movement in costs from the introduction in AESCSF V2

137. A potential source of cost increase is the updated (V2) of the AESCSF. For example, additional practices are likely to be included in V2 and require extra effort and/or tools to develop and embed.

138. To the extent that any such requirements are not already accounted for, we assume Endeavour Energy will either take AESCSF V2 into account in its revised RP or through a pass-through.

4.6.2 Timing

Timing of the initiatives is reasonable, and the implementation risk appears to be manageable

139. Endeavour Energy has provided a roadmap for the collection of IB3 programs, a description of the implementation (delivery) risks, the mitigating controls, and its resourcing strategy.

140. The cybersecurity projects are active for the entirety of the next RCP with the exception of '*Working with secure suppliers and partners*' (project 166) which is earmarked to commence in FY27. The level of effort required is not denoted in the roadmap which makes it difficult to assess the delivery risk, however given that Endeavour Energy only needs to implement [redacted] practices or less over 5 years, we consider that the delivery risk is likely to be manageable.

141. The sourcing strategy that Endeavour Energy describes[50] applies to all the initiatives/ projects under IB3 but many are applicable to cyber security implementation and all appear to be consistent with a balanced hybrid strategy (i.e. mix of internal and external resources).

142. The size of Endeavour Energy's cyber security team now and for achievement of SP-2 is not apparent from the documentation provided.

50

4.7 Our findings and implications

4.7.1 Summary of our findings

While not explicitly stated in its RP documentation, Endeavour Energy's cyber risk target appears to be appropriate

143. Endeavour Energy has compliance obligations arising from amendments to the SOCI Act and the Privacy Act, however, we infer that it has designed its project to extend beyond its minimum regulatory compliance obligations. Its cyber security investment strategy is predicated on maintaining the risk level 'stable' during the next RCP and which we consider to be appropriate. Whilst the information is not in its RP, Endeavour Energy has advised us that it has adopted the SP-2 AESCSF maturity target as its objective for the next RCP, and which we consider appropriate given its risk profile.

While presentational issues hamper critical assessment, we nevertheless consider that Endeavour Energy's proposed program is reasonable for a DNSP of its level of criticality

144. The combination of the following issues has led to significant challenges in assessing its proposed expenditure from a bottom-up perspective:

- Bundling of the cyber security options and options analysis with other 'resilience work' which masks the justification for the cyber security component;
- Conflicting information about the projects and the scope of the projects in various documents; and
- A flawed cost-benefit model which does not allow the relative merits of the six cyber security projects to be assessed.

145. Despite these issues with Endeavour Energy's presentation of what it proposes, we consider that a program of around the level that Endeavour Energy has proposed is reasonable for a DNSP of its level of criticality.

Except for inclusion of a capex contingency, Endeavour Energy's forecast cost is reasonable

146. Endeavour has added contingency amounts to the project which we consider is not warranted at a project level in an RP proposal because over the entire portfolio such contingencies should balance out. Apart from this, we consider Endeavour Energy's proposed capex is reasonable, being based on a reasonable methodology and supported by an external assessment.

4.7.2 Implications of our findings for proposed expenditure

We propose an alternative capex allowance of $13.1m

147. Based largely on our experience, Endeavour Energy's own benchmarking study, and its (likely) relatively small gap to SP-2 at the start of the next RCP, we consider that after removal of the proposed capex contingency allowance, the proposed capex is appropriate.

148. Noting that Endeavour Energy has not sought an opex step change, this results in an alternative capex allowance of $13.1m, as shown in Table 4.1. Consistent with Endeavour's proposal (as shown in Table 3.1), we propose that the adjusted amount would be spread evenly across the five years.

Table 4.1: EMCa's adjustment of Endeavour Energy's proposed cyber security expenditure ($m, 2024)

	END proposed [1]	EMCa adjustment [2]	Adjusted
Capex	16.30	-3.2	13.10

Notes: [1] Investment Brief 3, Tables 7 and 8, [2] Adjustment is from removal of Endeavour's proposed contingency amount, which is shown as $3,2m in Table 7 in its Investment Brief 3