

EMC^a

energy market consulting associates

Essential 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 Essential 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 Essential 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 Essential 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 from Cesare Tizi and Eddie Syadan

Date saved

26/09/2023 3:58 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

ABBREVIATIONS V

1 INTRODUCTION.....1

 1.1 Objective of this report.....1

 1.2 Scope of requested work.....1

 1.3 Our review approach1

 1.4 About this report5

2 RELEVANT CONTEXT TO OUR ASSESSMENT7

 2.1 Cyber security threat in Australia7

 2.2 Critical infrastructure - changes to regulation.....8

 2.3 The Australian Energy Sector Cyber Security Framework (AESCSF) 10

 2.4 AER Guidelines for non-network ICT assessment..... 12

 2.5 Implications for our assessment..... 13

3 ESSENTIAL ENERGY’S PROPOSED ICT CYBER SECURITY EXPENDITURE..... 15

 3.1 Overview and summary of proposed expenditure..... 15

 3.2 Summary of the basis for Essential Energy’s proposed expenditure 15

4 OUR ASSESSMENT..... 18

 4.1 Essential Energy’s risk analysis 18

 4.2 Essential Energy’s cyber-related objectives..... 19

 4.3 Essential Energy’s options analysis..... 20

 4.4 Essential Energy’s scope of work and cost forecasting methodology 22

 4.5 Other aspects..... 28

 4.6 Our findings and implications 29

LIST OF TABLES

Table 3.1: Essential Energy proposed SCS ICT cyber security related expenditures - \$million, real FY2024 15

Table 4.7: Assessment of scope and cost of Scope Item 7 (\$m, real 2024) 27

Table 4.8: EMCa’s adjustment of Essential Energy’s proposed cyber security expenditure (\$m, 2024)..... 29

LIST OF FIGURES

Figure 1.1: NER capital expenditure criteria2

Figure 1.2: NER capital expenditure objectives2

Figure 1.3: NER operational expenditure criteria3

Figure 1.4: NER operating expenditure objectives4

Figure 2.1: The cyber security problem8

Figure 2.2: AESCSF E-CAT criticality bands for electricity sector – TNSPs and DNSPs highlighted 11

Figure 2.3: Relationship between SPs, participant criticality , practices/anti-patterns and MILs – per AESCSF V1 11



ABBREVIATIONS

Term	Definition
ACM	Asset Change and Configuration Management
ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
Capex	Capital expenditure
CBA	Cost Benefit Analysis
CIAM	Customer Identity Access Management
CIRMP	Critical Infrastructure Risk Management Program
CPTX	Cyber Security Program 1,2, or 3
CRM	Customer Relationship Management
Current RCP	FY20-FY24
DNSP	Distribution Network Service Provider
E-CAT	Electricity Criticality Assessment Tool
ECSSO	Enhanced Cyber Security Obligations
EEMM	Essential Eight Maturity Model
FTE	Full-Time Equivalent
FY	Financial Year
ICT	Information and Communications Technology
IDAM	Identity Access Management
IT	Information technology
MIL	Maturity Indicator Level
NER	National Electricity Rules
Next RCP	FY25-FY29
NPC	Net Present Cost
NPV	Net Present Value
NSP	Network Service Provider
OT	Operational Technology
RCP	Regulatory Control Period
RMP	Risk Management Plan
RP	Revenue Proposal
SCS	Standard Control Services

Term	Definition
SLACI Act	Security Legislation Amendment (Critical Infrastructure) Act
SOCI Act	Security of Critical Infrastructure Act
SoNS	Systems of National Significance
SP	Security Profile
TNSP	Transmission Network Service Provider

1 INTRODUCTION

AER has asked us to review and provide advice on Essential Energy's proposed allowance for cyber security-related expenditure in the next Regulatory Control Period. Our review is based on information that Essential 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, Essential 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 Essential Energy's proposed cyber security-related capital expenditure ('capex') and step-change operating expenditure ('opex') included in Essential Energy's Revenue Proposal ('RP')
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 Decision on Essential Energy's revenue requirements for the next RCP.

1.2 Scope of requested work

4. The scope of this review covers Essential Energy's proposed allowance for:
 - Non-recurrent ICT cyber security capex; and
 - 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 Essential Energy to help ensure that we correctly understood the methodology and assumptions that Essential 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 Essential 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 Essential 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 Essential 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 Essential 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 Objectives and Criteria

12. The most relevant aspects of the NER in this regard 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) forecast capex and opex step change amount if it is satisfied that the capex and opex proposed reasonably reflects the expenditure criteria, and these in turn reference the expenditure objectives.
13. The NER 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 Distribution Network Service Providers (DNSP) 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 Essential Energy has proposed, our technical assessment framework is based on engineering considerations and economics.
18. We have sought to assess Essential Energy's expenditure proposal based on Essential Energy's analysis and Essential 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 Essential 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 Essential 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 Essential 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 Essential Energy has proposed for cyber security, as the basis for our assessment; and
 - In section 4, we describe our assessment of Essential Energy's proposed cyber security allowance, our findings on the prudence and efficiency of that allowance and the implications of those findings for the expenditure allowance that Essential Energy has proposed.

1.4.2 Information sources

21. We have examined relevant documents that Essential 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 by AER staff 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 Essential 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.

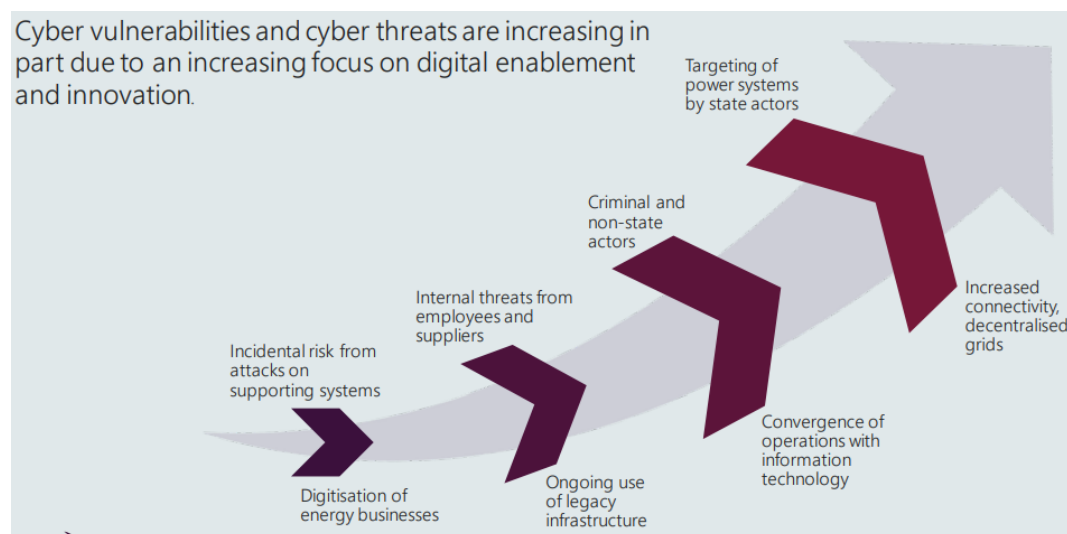
2 RELEVANT CONTEXT TO OUR ASSESSMENT

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 selects the EEMM as its cyber security framework.

2.2.3 Privacy Act amendments 2022⁸

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?bld=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

41. In response to an Information Request,¹⁰ Essential Energy provided a copy of the Instrument of Variation that applies to Essential Energy as a Licence Holder, dated 5 February 2019. Of relevance are the Critical Infrastructure Licence Conditions 9 (Substantial presence in Australia), 10 (Data Security), and 11 (Compliance) of the Licence. Within these conditions there are multiple requirements. 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 C2M2¹² 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)

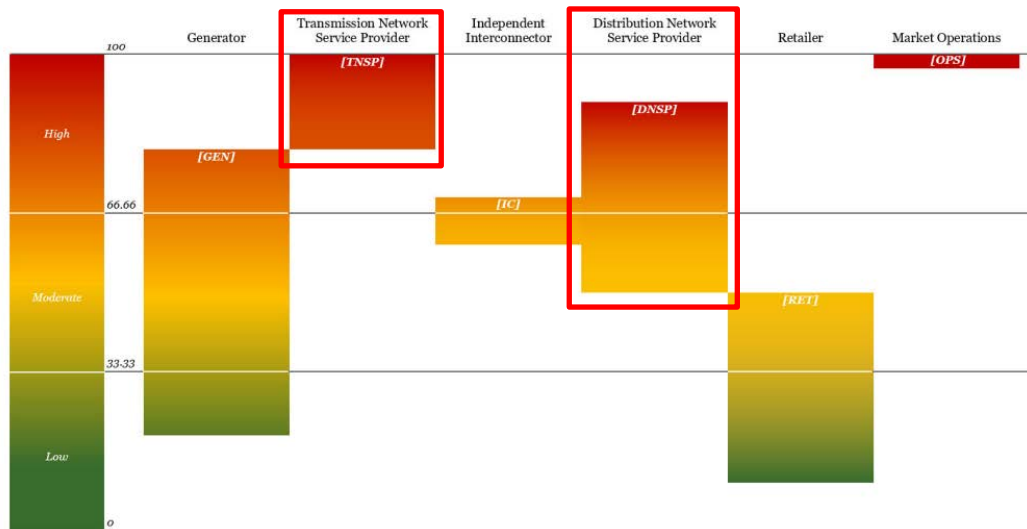
¹⁰ Essential Energy - IR020 Licence Conditions Variation - 20230512 - Confidential

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 ACM¹⁶ 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 DCCEE 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

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

2.4.1 Assessment of non-recurrent ICT capex

51. The AER's 2019 Non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to Essential Energy's proposed cyber security capex.
52. The AER requires DNSPs to allocate their non-recurrent ICT expenditures into the three subcategories for which it applies different assessment approaches: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 prudence) 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 providers [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 achieves benefits that are qualitative or intangible, we would expect evidence to support the*

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

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 prudence 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 Essential 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 ECSOs 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 \$2.22m to \$50.0m (maximum) with the expectation from the Federal government via the amendment that organisations such as Essential Energy will act accordingly to 'undertake robust privacy and security practices' which we interpret to include cyber security-related practices.
64. We have assessed how Essential Energy has responded to its common and specific cyber security compliance obligations, cognisant of:

²⁰ AER, Expenditure Forecast Assessment Guideline for Electricity Distribution, page 11

- 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 Essential 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. Given that the Instrument of Variation was provided to Essential Energy in early 2019, we consider that it 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 arising from the variations.

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

67. AESCSF V1 was the current version when Essential 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 Essential 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 Essential 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 Essential 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 Essential 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 ESSENTIAL ENERGY'S PROPOSED ICT CYBER SECURITY EXPENDITURE

Essential Energy has proposed a capex allowance of [REDACTED] for the next RCP. It has not proposed an opex step change.

3.1 Overview and summary of proposed expenditure

- 71. Essential Energy has proposed SCS cyber security-related ICT capex of [REDACTED], as shown in Table 3.1.²²
- 72. In Table 3.1 we also show Essential Energy's forecast of its opex expenditure, since this provides a more complete picture of its forecast level of effort. However, Essential Energy has not proposed a cyber-security related opex step change and therefore this does not form part of our assessment.

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

Description	2025	2026	2027	2028	2029	Total
Proposed Non-recurrent ICT- cyber security related capex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Forecast cyber-related opex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
TOTAL forecast cyber-related expenditure	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: IR#020 – ICT and Cyber Security – 20230512 - Confidential

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

- 73. Essential Energy has provided a business case and supplementary information to support its proposed program of investment for cyber security resilience and compliance for the next RCP.

3.2.1 Problem definition and risk assessment²³

- 74. Essential Energy advises that its Cyber Security Strategy is to 'achieve a "whole of organisation" cyber security maturity uplift through targeted investments and a clear cyber security roadmap.' The proposed investment program for the next RCP is designed to respond to the following drivers:

- **Compliance and Risk:** this addresses the risk of non-compliance with existing or future legislative and other obligations due to technology or capability limitations;
- **Business Improvement:** [REDACTED]

²² In Essential Energy's business case and costing analysis, this is referred to as [REDACTED]. This figure comprises the SCS and ACS components. Consistent with IR#020, the SCS CAM rate is of the order of 15%, which explains the difference.

²³ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 2

- **Productivity Improvement:** via digital automation in areas such as remediation of cyber security vulnerabilities, ICT system response and recovery, deployment of ICT infrastructure, and reporting for security and privacy compliance.

3.2.2 Essential Energy’s cyber security current state

75. Essential Energy reports that in the current RCP it is:²⁴

[REDACTED]

‘...building on its established Cyber Security Strategy, which describes how the company will achieve a “whole of organisation” cyber security maturity uplift through targeted investment and a clear cyber security roadmap.’

76. Essential Energy’s November 2022 cyber security rating was [REDACTED]²⁵ Based on the evidence provided by Essential Energy, its Cyber Security Program Tranches 1 and 2 (CPT1, CPT2) will achieve the following outcomes [REDACTED]

- [REDACTED]
- [REDACTED]

77. In response to an information request, Essential Energy confirmed that its current ‘Cyber Operating Model’ comprises [REDACTED]

78. Essential Energy has spent [REDACTED] to date on CPT1 and CPT2. The latter has a [REDACTED] budget. Together CPT1 and CPT2 will provide a solid foundation for what Essential Energy refers to as CPT3 for the next RCP, and which we take into account in assessing the risk controls and proposed expenditure for this period.

3.2.3 Options considered by Essential Energy for managing cyber security obligations and risks

79. Essential Energy considers a base case and two options:²⁹

- **Base Case -** [REDACTED]
- **Option 1: Invest in cyber security** [REDACTED]
- **Option 2: Invest in cyber security** [REDACTED]

²⁴ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 2

²⁵ Essential Energy AER EMCa Onsite Day 1 Confidential, slide 124

²⁶ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 7

²⁷ Essential Energy - IR020 Cyber Security Strategy Review Summary 2022 - 20230512 – Confidential, slides 4 and 5

²⁸ Essential Energy - IR020 ICT and Cyber Security - 20230512 – Confidential, pages 16-17

²⁹ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 2

80. Essential Energy has adopted Option 1 at a total cost of [REDACTED] over the next RCP, comprising [REDACTED] capex and [REDACTED] opex. For SCS, the proposed capex associated with option 1 is [REDACTED], and Essential Energy has not submitted for an opex step change.³⁰

³⁰ Essential Energy – 2024-29 Regulatory Proposal – Jan23-Public, page 65

4 OUR ASSESSMENT

We consider that Essential Energy’s cyber security program objectives and targets are appropriate, as is its risk prioritisation-based approach. We consider that one aspect of its proposed expenditure is overstated, but that the remainder of its proposed capex allowance is adequately supported and represents a reasonable allowance.

4.1 Essential Energy’s risk analysis

81. Essential Energy has provided a qualitative risk assessment in its business case. In this section we assess whether the risk analysis is sufficiently compelling to support the proposed cyber security investment in the next RCP. Essential Energy’s risk analysis also provides a framework for determining the appropriateness of its selected option for mitigating the risks, which we consider in section 4.3.

Essential Energy provides a satisfactory case for responding to the likely increase in cyber security risk over the next RCP

82. Essential Energy includes in its business case two themes affecting its cyber security over the next RCP that align with the issues raised in Section 2:

- **Deteriorating cyber threat landscape** – Essential Energy recognises that cyber security attacks are increasing in sophistication and volume.

[REDACTED]

[REDACTED]

[REDACTED]

83. Essential Energy has recognised and summarised adequately the basis for assessing that there would be an increasing likelihood of successful cyber-attacks and increasing consequences of a successful attack in the absence of further uplift in its cyber maturity.

Essential Energy identifies its cyber security-related compliance obligations

84. Essential 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 and the CIRMP Rules) and which it notes *‘further enables the introduction of future obligations regarding cyber security capability maturity, reporting and other controls, which are likely to come into effect within the coming RCP’*;³³ and
 - The NSW electricity distributor licence conditions and to the Privacy Act.
85. Essential Energy concludes that:³⁴

³¹ Australian Cyber Security Centre

³² Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 6

³³ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 9

³⁴ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 9

'Given the rapid growth in cyber security attacks in Australia in 2022, and the fragile international security environment, there is every reasonable expectation that the regulatory environment will continue to evolve to match these quickly developing cyber security threats.

[REDACTED]

4.2 Essential Energy's cyber-related objectives

Cyber security recognised as a strategic priority

87. [REDACTED]

[REDACTED]

Essential Energy has designed its project not only to comply with its minimum regulatory obligations, and its additional objectives provide a sound basis for the program

88. Essential Energy's objectives are not explicit in its business case, however from a table in section 1.2 (Corporate Strategy Alignment) combined with the risks it is seeking to control, we infer that its objectives can be summarised as:

- Maintain organisational compliance; and
- Lift capability to:
 - improve business processes and functions for greater security and resilience; and
 - enable productivity improvement.

89. We are satisfied that these objectives are aligned to its corporate strategy and provide a sound basis for developing its proposed response.

[REDACTED]

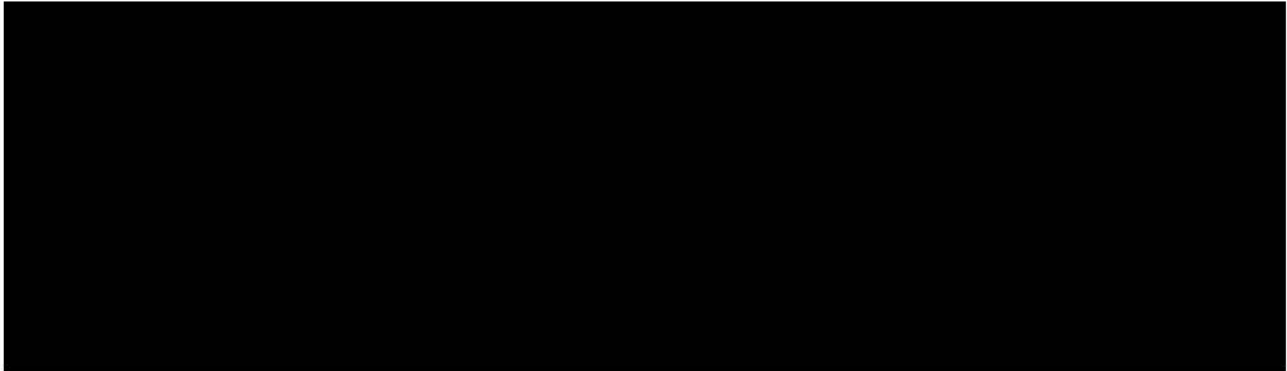
90. Essential Energy's strategy seems to be summarised as:³⁷

³⁵ [REDACTED]

³⁷ Essential Energy AER EMCa Onsite Day 1 Confidential, slide 109

'We'll build on our existing cyber security defences, with a coordinated program to ensure compliance with regulatory obligations, and to maintain a prudent residual risk position.'

91. The measures of success are shown in the figure below:



92. Essential Energy notes that *'according to the AEMO AESCSF guidance we should progress towards SP-2 to SP-3'*. Essential Energy states its objective for the next RCP as follows:



93. We assess how Essential Energy has applied its *'prudent risk-based approach'* in our review of its option analysis.

4.3 Essential Energy's options analysis

94. Essential Energy considers three options as recorded in its business case. We discuss the merits of each below.

4.3.1 Option 0 – 'Do nothing'³⁹

Option 0 is predicated on making no further investment to support cyber security risk migration

95. The cost of Option 0 over the next RCP is nil. Option 0 is positioned as the counterfactual for Options 1 and 2 and as such the avoided cost of a cyber security breach(es) during the next RCP is credited to those options as a benefit compared to Option 0, rather than including it as a dis-benefit for Option 0. This is an appropriate specification and we therefore discuss Essential Energy's derivation of the dis-benefit as part of our assessment of Option 1.

96.

Essential Energy reasonably concludes that this option is not prudent

97.

³⁸ Essential Energy AER EMCa Onsite Day 1 Confidential, slide 128

³⁹

[REDACTED]

4.3.2 Option 1 - [REDACTED] (Recommended by Essential Energy)

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED] Nonetheless, Essential Energy's strategy has merit, particularly given (i) the timing of its RP development/submission, (ii) seeking to achieve value for money [REDACTED], and (iii) uncertainty about ongoing regulatory obligations, their impact, and cost to comply.

4.3.3 Option 2 – [REDACTED]

[REDACTED]

103. Option 2 adds two additional scopes of work to Option 1 [REDACTED]

- [REDACTED]

- [REDACTED]

104. The estimated incremental totex compared to Option 1 is [REDACTED] (whole-of-business) and [REDACTED]

Essential Energy reasonably concludes that this option is not prudent

105. [REDACTED] Option 2 it is not Essential Energy's preferred option and we concur with its conclusion, [REDACTED]

[REDACTED]

4.4 Essential Energy’s scope of work and cost forecasting methodology

4.4.1 Summary

Essential Energy’s cost forecasting methodology appears to be appropriate but we have issues with some aspects of the scope

106. In response to an information request, Essential Energy provided its Estimation Worksheet, which we have used to help assess its cost forecasting methodology and the reasonableness of its input assumptions. We conclude that Essential Energy’s cost forecasting methodology follows common practice, which in Essential Energy’s case we summarise as follows:⁴¹

- 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 differentials between planned resourcing mix (i.e. hybrid insource/outsource model) is accounted for;
- Forecast labour costs are based on typical unit rates / day rates;
- Essential Energy has not explicitly included project level contingency amounts; and
- It has incorporated external advice to both help define the scope and the cost estimates.

107. We consider that Essential Energy’s cyber resilience cost forecasting methodology is appropriate, however we have concerns with certain scope items which we consider to be inappropriate and which lead, in aggregate, to a cost over-estimate.

Essential Energy is not seeking an opex step change and its business case covers whole-of-business costs, which are later allocated between SCS and ACS

108. Essential Energy’s business case seeks to justify [REDACTED] one-off opex (including [REDACTED] [REDACTED] and [REDACTED] recurrent opex.⁴² However, Essential Energy is not seeking an opex step change from Option 1 (its recommended option).

109. Because business cases appropriately consider all costs, we refer extensively to totex and opex in the following sections. However, our assessment is necessarily of what Essential Energy has proposed in its SCS RP, which is solely a capex allowance as described in section 3.

4.4.2 Definition of scope items by reference to Essential Energy’s objectives

The project objectives are consistent with Essential Energy’s risk assessment

110. Essential Energy’s CPT3 (per Option 1) is built around five key ‘Scope Items’ as they are referred to by Essential Energy, as follows:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

⁴¹ Essential Energy AER EMCa Onsite Day 1 Confidential, slide 130

⁴² These amounts are as per Essential Energy’s business case. This comprises costs which are later allocated between SCS and ACS, as per Essential Energy’s CAM. Assessment of its CAM allocations is not within our scope. Our eventual assessment is of the SCS capex allowance that Essential Energy has proposed.

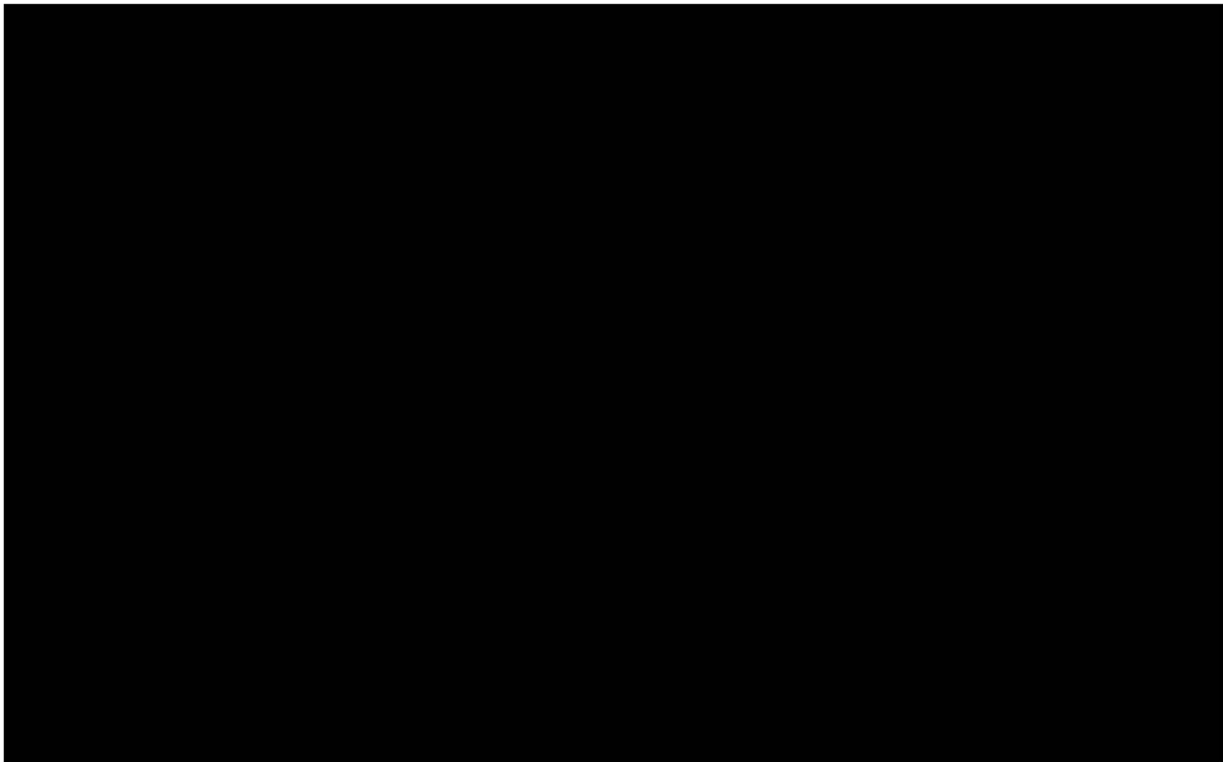
- [REDACTED]
111. These Scope Items and the objectives of each, are directly aligned to Essential Energy's strategy and overarching objectives.
112. Essential Energy has also included the following three 'overarching' Scope Items in Option 1, which form part of its costing, as follows:
- [REDACTED]
 - Scope item 7: Program delivery; and
 - Scope item 8: CPT2 Program Labour (FY25).

4.4.3 Assessment of scope and cost of each scope item⁴³

Scope Item 1: [REDACTED]

The proposed capex for scope item 1 is reasonable

113. [REDACTED]
- [REDACTED]



⁴³ As per section 3.2.3, the costs in this section are for the whole business, whereas Essential Energy has proposed the SCS component

⁴⁴ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, pages 15-17

Scope Item 2: [REDACTED]

[REDACTED] we consider that its proposed cost for this is overstated

115. [REDACTED]

[REDACTED]

116. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] we have not seen adequate justification for this from a risk-cost perspective, particularly given Essential Energy's own risk analysis. However, we also note that Essential Energy is not claiming an opex step change in its RP for its cyber security program.

120. Whilst Essential Energy does not explicitly denote a project dependency with its proposed CRM and Portal non-network ICT project, we note that the project costs [REDACTED]

[REDACTED] We have separately assessed⁴⁹ that Essential Energy has not adequately justified its investment in the CRM/Portal project. We therefore consider that there is an interdependency between the CRM/Portal project and [REDACTED] of this Scope Item and that in the absence of the former, the cost of [REDACTED] may be reduced, even to zero.

⁴⁵ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, pages 17-19
⁴⁶ Including by reference to the response to IR020: Essential Energy - IR020 Cyber Security Resilience Estimation Worksheet - 20230512 – Confidential, Detailed Projects and Costing
⁴⁷ Essential Energy - IR020 Cyber Security IDAM Strategy and Roadmap - 20230512 – Confidential, slide 8
⁴⁸ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 18
⁴⁹ EMCa report to AER on Essential Energy 24-29 DER and ICT

121. We have also considered the costs for [REDACTED] proposed by other NSPs as part of their compliance and cyber security maturity plans as a means of benchmarking Essential Energy's proposed [REDACTED] totex and find that it is between 40%-60% more expensive.⁵⁰ We assume the majority of this cost difference is due to Essential Energy's [REDACTED]

122. We consider that the [REDACTED] is also overstated, but by around [REDACTED]

123. We therefore conclude that:

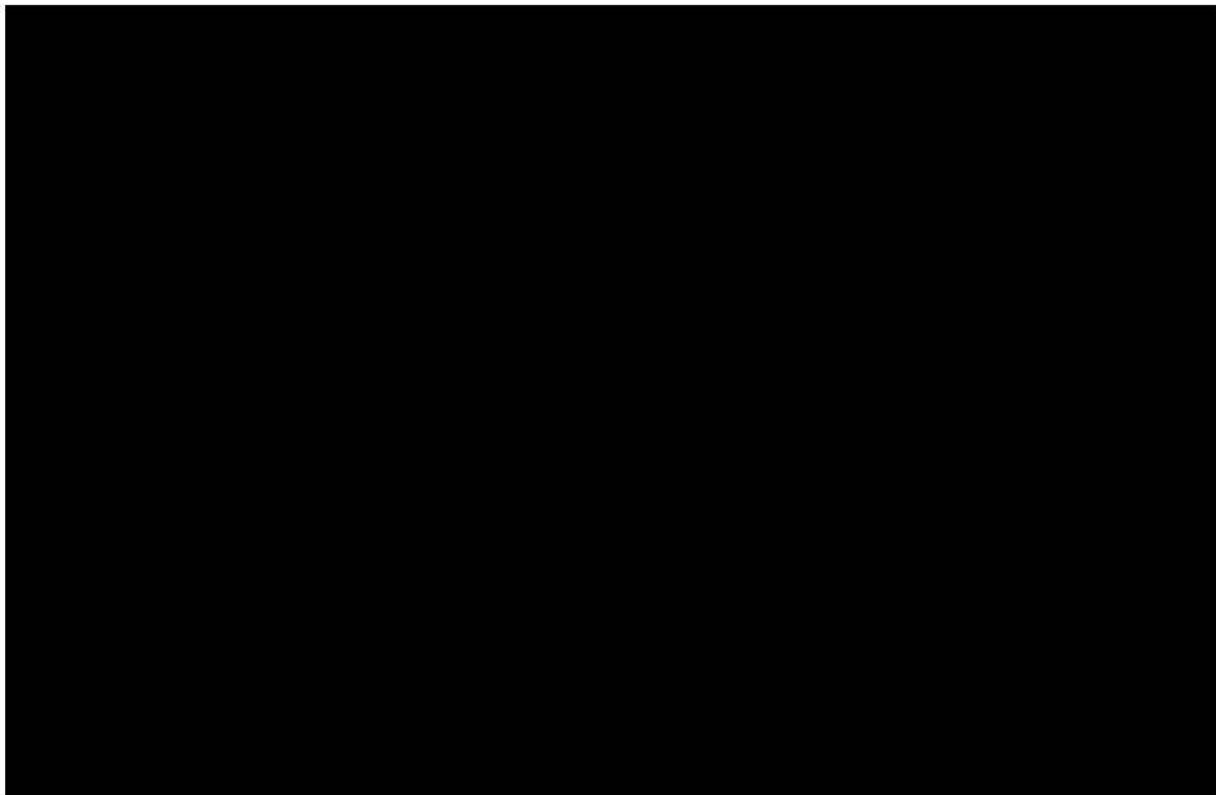
- Essential Energy's [REDACTED] capex expenditure is likely to be high, given that we do not consider that Essential Energy has adequately demonstrated that spending to [REDACTED] and considering our experience and benchmarking results; and
- Essential Energy's [REDACTED] may not be a prudent investment given that it appears to be a business initiative with questionable value for money given the incremental cost and the link to what we consider to be an unjustified CRM/Portal project.

Scope item 3: [REDACTED]

For this scope, Essential Energy has not proposed a capex allowance

124. [REDACTED]

125. The table below summarises our assessment of the proposed expenditure.



⁵⁰ [REDACTED]

⁵¹ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, pages 19-21

Scope Item 4: [REDACTED]

The proposed capex for scope item 4 is reasonable

126.

[REDACTED]

Scope Item 5: [REDACTED]

For this scope, Essential Energy has not proposed a capex allowance

127.

128. Our assessment is summarised in the table below.

[REDACTED]

Scope Item 6: [REDACTED]

For this scope, Essential Energy has not proposed a capex allowance

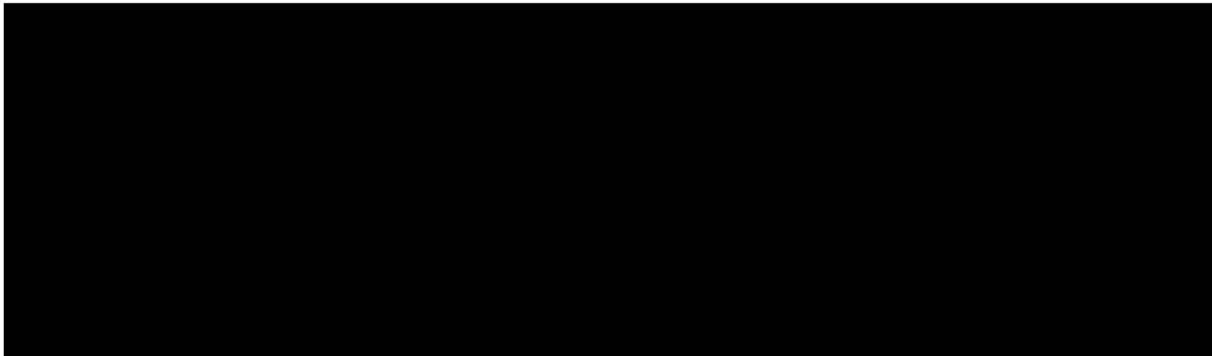
129.

130. Our assessment is summarised in the table below.

⁵² Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, pages 21-22

⁵³ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, pages 22-23

⁵⁴ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 23



Scope Item 7: Program delivery⁵⁵

For this scope, Essential Energy has not proposed a capex allowance

- 131. The objective of this scope item is '[e]nsure the efficient delivery of the Cyber Security program, by engaging specialist project delivery resources to apply program and project disciplines.'
- 132. Our assessment is summarised in the table below.

Table 4.7: Assessment of scope and cost of Scope Item 7 (\$m, real 2024)

Workstream	Capex	Opex one-off	Opex - recurrent	EMCa assessment
Program management resourcing/function to oversee CPT3 delivery.	■	■	■	The program management resourcing/function is approx. ■ of the totex, which we consider to be reasonable

Source: Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 24

Scope item 8: CPT Program Labour (FY25)

For this scope, Essential Energy has not proposed a capex allowance

- 133. Essential Energy has included ■ opex in its proposed opex of ■ for Option 1 without explanation.⁵⁶ However, since Essential Energy has not sought an opex step change, we have not sought further information on this amount and its justification.

4.4.4 Potential cost movement

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

- 134. A potential source of cost increase is the updated (V2) of the AESCSF. For example, additional practices are likely to be included in V2.
- 135. To the extent that any such requirements are not already accounted for, we assume Essential Energy will take AESCSF V2 into account in its revised RP or via a pass-through.

⁵⁵ Essential Energy – 10.07.02 Cyber Security Investment Case (corrected) – 20230512 - Confidential, page 24

⁵⁶ We can see no explanation in its business case nor in the NPV model nor in the Estimation Worksheet provided in response to information request IR020.

4.5 Other aspects

4.5.1 Economic justification

Essential Energy has not sought to quantify a benefit from avoided security breaches

136. As discussed elsewhere, because we consider that the totex proposed by Essential Energy is primarily directed towards maintaining the risk level, not improvement, it is not strictly necessary for it to demonstrate a positive NPV for its project.
137. Essential Energy has provided a NPV worksheet, but it has not included an avoided cyber breach ('risk abatement') benefit. Based on our experience, if a significant cyber-attack is successful:
- The cost to sanitise and re-build the affected systems, including the forensic analysis, and resetting would be in the range [REDACTED] for a business of Essential Energy's size and complexity;
 - Cost to remediate security gaps would be in the order of [REDACTED];
 - Whilst there may be a ransom request, we have not factored this in on top of the above range estimates;
 - Whilst there may be loss of revenue, we have not factored this in on top of the above range of estimates; and
 - [REDACTED]
138. Therefore, we consider that it would be reasonable to assume:
- A risk abatement benefit in the range [REDACTED] over 5 years or [REDACTED] over a 10 year CBA study period; and that
 - For the purposes of CBA modelling, a midpoint estimate of [REDACTED] or [REDACTED] would be reasonable.
139. Based on this benchmark guide, Essential Energy's totex cost estimate of [REDACTED] (SCS) is at the high end of a reasonable range, but it is not unreasonable. It provides a ball-park economic validation of Essential Energy's proposed expenditure; also its choice of Option 1 as opposed to Option 0 (by reference to the benefits that would be forgone with this option) or Option 2 (by reference to its considerably higher cost).

4.5.2 Timing

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

140. Essential Energy has provided a completion timeframe for its project and a detailed description of the implementation (delivery) risks, including the mitigating controls. In aggregate, there are manageable risks to completing the project within the next RCP, with the residual risk rating (i.e. after mitigating controls are applied) [REDACTED] which we consider to be a reasonable assessment.

4.6 Our findings and implications

4.6.1 Summary of our findings

Essential Energy’s cyber project objectives and risk targets are appropriate

- 141. Essential Energy has compliance obligations arising from amendments to the SOCI Act, the Privacy Act, and the NSW Distributor’s Licence, however, it has designed its project to not only comply with its regulatory obligations. In addition, we infer its cyber security investment strategy is predicated on [REDACTED] during the next RCP.
- 142. In accordance with the AER ICT capex assessment guidelines, we have therefore considered the prudence and efficiency of Essential Energy’s proposed cyber security forecast to address broader risk than its compliance obligations.

Essential Energy’s ‘prudent risk-based approach’ is appropriate

- 143. Essential Energy has adopted a ‘prudent risk-based approach’ [REDACTED], which we consider appropriate for Essential Energy given its risk profile.

We consider that Essential Energy’s proposed [REDACTED], which comprises almost all of its proposed capex, is overstated

- 144. Essential Energy’s proposed cyber security capex is [REDACTED]. From our experience and from comparison with peer organisations’ similar [REDACTED] costs, Essential Energy’s proposed cost for work of this nature is higher than is likely to be required.

While we have provided some observations on Essential Energy’s forecast opex, it is not within our scope to assess it as Essential Energy has not proposed an opex step change for this

- 145. Essential Energy has not sought an opex step change in its RP for its cyber security program, noting that it has already established [REDACTED]

4.6.2 Implications of our findings for proposed expenditure

- 146. In Table 4.8 we summarise our proposed adjustment to the capex allowance that Essential Energy has sought, which is based on a correction for what we consider to be an excessively high investment [REDACTED] and which comprises almost all of Essential Energy’s proposed capex. Based on our experience and comparative analysis for this project, we consider an adjustment of [REDACTED] is likely to result in a prudent level of cyber security capex for the next RCP.

Table 4.8: EMCa’s adjustment of Essential Energy’s proposed cyber security expenditure (\$m, 2024)

	Essential Energy Proposed	EMCa proposed adjustment	EMCa proposed Adjusted	% of Essential Energy proposed
Capex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]