

EMC^a

energy market consulting associates

CitiPower, Powercor and United Energy ('CPU') 2026 - 2031
Regulatory Proposals

REVIEW OF PROPOSED EXPENDITURE ON CYBER SECURITY



Report prepared for:
**AUSTRALIAN ENERGY
REGULATOR (AER)**
August 2025

Preface

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

This report covers a particular and limited scope as defined by the AER and should not be read as a comprehensive assessment of proposed expenditure that has been conducted making use of all available assessment methods nor all available inputs to the regulatory determination process. This report relies on information provided to EMCa by the CPU business entities. 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 overarching purpose.

Except where specifically noted, this report was prepared based on information provided to us prior to 1 June 2025 and any information provided subsequent to this time may not have been taken into account. Some numbers in this report may differ from those shown in the CPU business entities' regulatory submissions or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell

Managing Director
psell@emca.com.au

Prepared by

Mark de Laeter, Paul Sell and Eddie Syadan

Date saved

23/09/2025 4:38 PM

Version

Final v1

Energy Market Consulting associates

ABN 75 102 418 020

Sydney Office

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

Perth Office

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

CONTENTS

ABBREVIATIONS	V
1 INTRODUCTION.....	1
1.1 Purpose of this report.....	1
1.2 Scope of requested work.....	1
1.3 Our review approach	1
1.4 This report.....	5
2 REVIEW OF PROPOSED CYBER SECURITY EXPENDITURE	7
2.1 Introduction	7
2.2 Background and context	7
2.3 Overview and summary of proposed expenditure	8
2.4 Assessment	9
2.5 Summary of our findings and implications for CPU’s proposed cyber security expenditure.....	15
APPENDIX A CYBER SECURITY BACKGROUND AND CONTEXT INFORMATION	17
APPENDIX B RELEVANT AER GUIDELINES FOR ASSESSMENT OF ICT EXPENDITURE	22

LIST OF TABLES

Table 2.1: CPU’s proposed cyber security expenditure - \$m, real 2026	9
Table 2.2: Recurrent historical cyber security totex – FY22 – FY26 (\$m, 2026)	11
Table 2.3: Selected CPU input assumptions for ‘customer loss of supply due to cyber-attack’ risk derivation	15

LIST OF FIGURES

Figure 1.1: NER capital expenditure criteria	2
Figure 1.2: NER capital expenditure objectives	3
Figure 1.3: NER operating expenditure criteria	3
Figure 1.4: NER operating expenditure objectives	4
Figure 2.1: Threat scenarios.....	10
Figure 2.2: CPU’s cyber security focus areas for the current RCP and AESCSF self-assessment results.....	10
Figure 2.3: Proposed expansion of CPU’s cyber security team	13
Figure 2.4: CP + PAL + UE cyber security expenditure forecast – Option 2 (\$2024).....	14

ABBREVIATIONS

Term	Definition
ACSC	Australian Cyber Security Centre
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
ASD	Australian Signals Directorate
BR1	Business Risk 1
C2M2	Cyber Security Maturity Model
Capex	Capital expenditure
CBA	Cost Benefit Analysis
CER	Customer Energy Resources
CIRMP	Critical Infrastructure Risk Management Program
CPU	CitiPower, Powercor, and United Energy
Current RCP	2022-2026 RCP
DNSP	Distribution Network Service Provider
E-CAT	Electricity Criticality Assessment Tool
ECISO	Enhanced Cyber Security Obligations
EEMM	Essential Eight Maturity Model
FTE	Full Time Equivalent
ICT	Information and Communication Technology
IR	Information Request
IT	Information Technology
MIL-1	Meeting Maturity Indicator Level One
NER	National Electricity Rules
Next RCP	2027-2031 RCP
NPV	Net Present Value
NSP	Network Service Provider's
Opex	Operational expenditure
OT	Operational Technology
PAL	Powercor
RCP	Regulatory Control Period

Term	Definition
RP	Regulatory Proposal
SCS	Standard Control Service
SOCI Act	SOCI Act (The Security of Critical Infrastructure Act 2018)
SP	Security Profile under the AESCSF
UE	United Energy
TOTEX	Total expenditure

1 INTRODUCTION

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

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

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

1.1 Purpose of this report

1. The purpose of this report is to provide the AER with a technical review of aspects of the expenditure that CitiPower, Powercor, and United Energy (collectively 'CPU') have proposed in their respective regulatory proposals (RP) for next RCP.
2. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed expenditures allowance as an input to its Draft Determination on the three DNSPs' revenue requirements for the next RCP.

1.2 Scope of requested work

3. Our scope of this review, as requested by the AER, covers both ex-ante capex and opex step changes related to ICT cyber security.
4. Because of similarities between the three business cases¹ and Excel models in support of CPU's cyber security expenditure, we have presented one report for the three DNSPs but we have taken into account any differences that may affect our findings.
5. Other aspect of CPU's expenditures, including repex, augex, opex (vegetation management), CER and other ICT related expenditures are covered in our four other reports.

1.3 Our review approach

6. In conducting this review, we first reviewed the documents that CPU submitted to the AER as part of its proposal for the next RCP. This includes Excel models which are relevant to our scope.
7. We next collated several information requests. The AER combined these with information request topics from its own review and sent these to CPU.
8. In conjunction with AER staff, our review team met with CPU at its offices on 2 – 4 April 2025. CPU presented to our team on the scoped topics, and we had the opportunity to engage with CPU to consolidate our understanding of its proposal.
9. CPU provided the AER with responses to information requests and, where they added relevant information, these responses are referenced within this review.

¹ CP BUS 6.02 - Cyber security - Jan2025; PAL BUS 7.02 – Cyber security – Jan2025; UE BUS 7.02 - Cyber security - Jan2025

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

1.3.1 Conformance with NER requirements

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 and relevant AER Guidelines.

Capex objectives and criteria

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

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

Figure 1.2: 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 do each of the following (**the capital expenditure objectives**):
- (2) meet or manage the expected demand for standard control services over that period;
 - (3) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;
 - (4) to the extent that there is no applicable regulatory obligation or requirement in relation to:
 - (i) the quality, reliability or security of supply of standard control services; or
 - (ii) the reliability or security of the distribution system through the supply of standard control services,
 to the relevant extent:
 - (iii) maintain the quality, reliability and security of supply of standard control services; and
 - (iv) maintain the reliability and security of the distribution system through the supply of standard control services;
 - (5) maintain the safety of the distribution system through the supply of standard control services; and
 - (6) contribute to achieving emissions reduction targets through the supply of standard control services.

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

Opex Objectives and Criteria

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

Figure 1.3: NER operating expenditure criteria

NER operating expenditure criteria

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

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

Figure 1.4: 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 do each of the following (the operating expenditure objectives):*
- (1) meet or manage the expected demand for standard control services over that period;*
 - (2) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;*
 - (3) to the extent that there is no applicable regulatory obligation or requirement in relation to:*
 - (i) the quality, reliability or security of supply of standard control services; or*
 - (ii) the reliability or security of the distribution system through the supply of standard control services,**to the relevant extent:*
 - (iii) maintain the quality, reliability and security of supply of standard control services; and*
 - (iv) maintain the reliability and security of the distribution system through the supply of standard control services; and*
 - (4) maintain the safety of the distribution system through the supply of standard control services; and*
 - (5) contribute to achieving emissions reduction targets through the supply of standard control services.*

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

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

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

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

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

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 CPU has proposed, our technical assessment framework is based on engineering considerations and economics.
18. We have sought to assess CPU's expenditure proposal based on CPU's analysis and CPU'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 CPU 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 CPU 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 CPU's RP documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 This report

1.4.1 Report structure

20. In following assessment section, we have presented:
- An overview of the proposed expenditure and a summary of CitiPower, Powercor and United Energy's justification for that expenditure
 - Our assessment of proposed cyber security expenditure, and
 - Our findings for proposed cyber security expenditure and the implications of the findings for the expenditure allowances determined by the AER in its Draft Determination.
21. We also provide the following appendices:
- Appendix A - Cyber security background, and
 - Appendix B - relevant AER Guidelines.
22. We have taken as read the considerable volume of material and analysis that CPU provided, and we have not sought to replicate this in our report except where we consider it to be directly relevant to our findings.

1.4.2 Information sources

23. We have examined relevant documents that CPU have published and/or provided to the AER in support of the areas of focus and projects that the AER has designated for review. This included further information at onsite meetings and further documents in response to

our information requests. These documents are referenced directly where they are relevant to our findings.

24. Except where specifically noted, this report was prepared based on information provided by AER staff prior to 30 May 2025 and any information provided subsequent to this time may not have been taken into account.
25. Unless otherwise stated, documents that we reference in this report are CPU documents comprising its RP and including the various appendices and annexures to that proposal.
26. We also reference responses to information requests, using the format IRXX being the reference numbering applied by the AER. Noting the wider scope of the AER's determination, the AER has provided us with IR documents that it considered to be relevant to our review.

1.4.3 Presentation of expenditure amounts

27. Expenditure is presented in this report in \$2025-26 real terms, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.
28. While we have endeavoured to reconcile expenditure amounts presented in this report to source information, in some cases there may be discrepancies in source information provided to us and minor differences due to rounding. Any such discrepancies do not affect our findings.

2 REVIEW OF PROPOSED CYBER SECURITY EXPENDITURE

CPU proposes \$38.0 million capex and \$37.6 million opex for cyber security in the next RCP.

CPU has established a significant cyber security capability in the current RCP and which, indirectly, its customers benefit from through both economies of scale and costs

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

CPU have collectively demonstrated that it understands its cyber security compliance obligations and the emerging and increasing cyber security threats and risks from a variety of sources.

We find that CPU's proposed strategy of maintaining a tolerable risk level over the course of the next RCP by using a risk-based approach to determine what new or enhanced controls it needs to adopt is appropriate.

Whilst in aggregate, the proposed expenditure for cyber security represents a significant uplift on expenditure in the current period, we consider that the capex proposed for each CPU business is reasonable and that the proposed opex step changes are reasonable estimates of incremental opex that each business will need to incur.

2.1 Introduction

- 29. CitiPower and Powercor (together) and United Energy have provided an Investment Briefs to justify an uplift in its cyber security capability over the next RCP in response to increasing cyber security threats.
- 30. Where relevant, we distinguish between CPU combined capabilities, analyses, initiatives and costs, and the individual businesses.
- 31. In this section we provide an overview of the expenditure proposed by CitiPower, Powercor and United Energy, that we have assessed in this report.

2.2 Background and context

- 32. In the appendix to this document, we provide background and context information on the cyber security threat landscape in Australia, relevant cyber security frameworks and obligations and their relevance to DNSPs.
- 33. In undertaking our assessment, we take account of the following factors.

Increasing threat landscape and attack surface mean cyber risk is increasing

34. The advice from government agencies is that the cyber-attack landscape is worsening. The 'digitisation' of electricity network operations, including into the low voltage networks with the proliferation of remote but connected devices means that the cyber-attack surface presented by NSPs is increasing, leading to an increasingly higher risk of cyber-attack and potential breach over time.
35. In our assessment we have sought to understand how CPU has incorporated the increasing threat landscape and attack surface issues into its risk analysis and, ultimately into its option selection and proposed expenditure profile.

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

36. 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, noting that SP-1 is the least onerous of the security profiles under the AESCSF.²
37. [REDACTED]
38. Further, the civil penalties for a breach(es) of the Privacy Act were increased in 2022 from \$2.2 million to \$50.0 million (maximum) with the expectation from the Federal government via the amendment that organisations such as CPU will act accordingly to implement and diligently apply robust privacy and security practices. We interpret these to include cyber security-related practices.
39. We have assessed how CPU 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.
40. We have also considered whether CPU has identified any other relevant obligations.
41. In addition to its minimum compliance obligations, we consider the controls CPU has proposed (and the cost of them) to manage the increasing cyber security threat landscape. A useful reference is the Security Profile (SP) practices expected to be in place by the end of the current RCP and the projected SP practices CPU is likely to achieve with the proposed investment by the end of the next RCP.

2.3 Overview and summary of proposed expenditure

2.3.1 What CPU has proposed in its RP

42. Table 2.1 below shows CPU's proposed capex and opex step changes for cyber security.
43. CPU proposes an uplift in expenditure in the next RCP to respond to increasing external cyber threats to IT systems and Operational Technology (OT) systems, which is exacerbated by the increasing attack surface area (dues to the increasing number of

² Australian Energy Sector Cyber Security Framework

³ System of National Significance

⁴ Enhanced Cyber Security Obligation

touchpoints that malicious actors may attempt to breach given digitalisation across the networks).

Table 2.1: CPU's proposed cyber security expenditure - \$m, real 2026

Project	CitiPower	Powercor	UE	Total
Capex	5.6	13.0	19.4	38.0
Opex (step changes)				
recurrent	4.5	10.4	14.9	29.8
non recurrent	1.2	2.7	3.9	7.8
subtotal opex	5.6	13.2	18.8	37.6
Total - cyber expenditure	11.2	26.2	38.2	75.6

Source: EMCa table derived from CPU's SCS Capex and Opex models

2.4 Assessment

44. In this section we assess the prudence and efficiency of CPU's proposed expenditure to sustaining its current level of cyber security capability and to enhance it through the next RCP to address forecast continuing escalation of cyber threats.
45. CitiPower and Powercor presents a combined business case with the proposed expenditure to manage cyber security risks presented in aggregate for the two businesses. United Energy presents a near-identical business case with the material difference being that the quoted expenditures are for United Energy alone. For all but the cost allocation, we have therefore assessed the 'group' cyber security strategy, objectives, risk assessment, and responses once and refer to the individual costs and benefits as required.

2.4.1 CPU's cyber security strategy and objectives

Increased cyber threat and compliance obligations are appropriately identified

46. In its business cases, CPU has adequately identified (i) its legislative obligations, (ii) the increasing cyber threat landscape, and (iii) its increasing cyber-attack surface area.
47. Along with its peers, CPU stresses the reliance of the electricity on IT and operating technology (OT) systems and data and the need for robust cyber security controls:⁵
- 'Malicious actors are increasingly targeting OT systems, such as supervisory control and data acquisition (SCADA) systems... The distributed energy resources spread across our network, the new inter-connected devices digitalising our grids, and the IT-OT convergence all increase our exposure points and the complexities of how we manage the breadth of threat entries.'*
48. This is further illustrated in the extract from CPU's on-site presentation shown in Figure 2.1:

⁵ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 8

Figure 2.1: Threat scenarios

	Threat	Vulnerability	Consequence
Threat Scenario	<p>A threat actor sends a well crafted phishing email with a malicious attachment.</p> <p>Our employee accidentally opens the attachment that creates a backdoor for the attacker to access our IT network.</p>	<p>The actor scans the IT network to discover IT assets with unpatched vulnerabilities. The attacker exploits these vulnerabilities, gains privilege access and moves through the network undetected, eventually reaching the OT network.</p> <p>The attacker continues to discover OT assets with unpatched vulnerabilities, or weak security controls.</p>	<p>The attacker deploys a malicious payload to disrupt the communication network, resulting in a SCADA screen blackout.</p> <p>The loss of visibility has potential impact to the availability and safety of the power network.</p>

Source: Extract from CPU's EMCa onsite workshops - cyber – final, slide 13

49. We are satisfied that not only is the reasonable view that the threat actors are becoming increasingly numerous and sophisticated, but CPU's attack surface area is expanding with the IT-OT convergence and distributed exposure points.

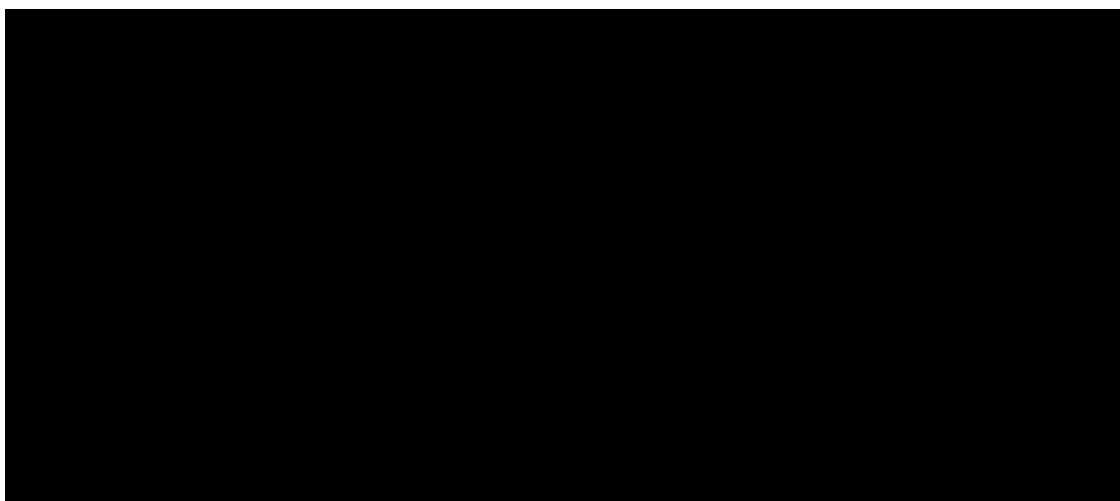
CPU's strategy is to enhance its cyber security capability to offset the worsening threat landscape

50. CPU's cyber security strategy is based on building on the foundational capability it has established in the current RCP to 'further enhance our capabilities and apply defences in depth to better protect our network and customers as the threat landscape evolves.'⁶
51. CPU proposes a risk-based approach to determining which controls and in what sequence to build them over the next RCP to enhance its capabilities. We consider a risk-based approach to be appropriate.

2.4.2 CPU's current state

CPU achieved SP-1+ (V2) as of late 2024

52. Figure 2.2 illustrates both CPU's focus areas at the start of the current RCP and the end-of-2024 self-assessment result, measured by practice count achieved across 11 AESCSF domains. CPU reports that it completed 268 practices, with a SP-1+ profile score against Version 2 (V2) of the AESCSF.⁷



⁶ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 23

⁷ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, pages 3, 4

Expected expenditure in the current period

53. In response to information requests, we were provided with the historical cost information summarised in Table 2.2 and advised that current cyber security opex requirements have been estimated to remain the same to sustain existing capabilities through the next RCP.⁸

Table 2.2: Recurrent historical cyber security totex – FY22 – FY26 (\$m, 2026)

Business	CitiPower	Powercor	United Energy	Total
Recurrent cyber security totex	14.5	30.1	32.9	77.5

Sources: CP response to IT016, q3, Table 4; PAL response to IR015, q3, Table 4; UE response to IR013, q, Table 4

54. CPU advises that:⁹
- It reprioritised the remaining cyber security activities in response to SOCI updates and following AEMO's release of AESCSF version 2.0 in October 2022, and
 - Its cyber security investments in the current period have focused on establishing 'foundational' capability, which has reduced its overall cyber security risk profile from 'extreme' to 'high'.
55. CPU presented no further quantitative or qualitative evidence to support the claim in its Business Case that its risk of cyber-attack is 'high' (i.e. despite its investment in the current RCP). We asked CPU for supporting evidence. It responded¹⁰ with monthly event data from which we are satisfied that there is evidence of escalating risk. Based on the evidence of escalating cyber risks, CPU's current maturity level, and the introduction of the AESCSF V2 (which essentially recognises the need for additional controls even for SP-1 level maturity), we consider that:
- It was prudent for CPU to take appropriate measures to build its cyber security capability in the current period
 - The areas of focus denoted in Figure 2.2 (per 2024 self-assessment) are appropriate, and
 - A risk level of 'high' for CPU (using the typical definitions of likelihood and consequence) at the commencement of the next RCP is reasonable.
56. We consider that CPU has adequately demonstrated that there is a need to continue to invest in expanding and deepening its cyber security controls over the next RCP.

2.4.3 CPU's cyber security options analysis

CPU considered three options and selected the prudent approach

57. CPU identified three options to respond to the identified need (risk assessment) and cognisant of its current cyber maturity level and SOCI Act obligations:
- Option 1: Maintain existing cyber security maturity - as CPU points out, this is not a 'do nothing' option – it is a 'do-nothing different' approach, maintaining existing capabilities (and therefore the SP-1+ level) by keeping controls up-to-date and to meet *known and anticipated legal and regulatory obligations*¹¹
 - Option 2: Enhance cyber security resilience capability – described by CPU as taking a risk-based approach to selecting the practices that will provide the most value to customers, based on a risk-reduction/cost balance but compatible with the 'maintaining' overall risk strategy, and

⁸ PAL response to IR008q5, and we note that Option 1 expenditure is \$18.0 million for CPU combined (i.e. for sustaining cyber maturity at the current level throughout the next RCP)

⁹ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, pages 3, 4

¹⁰ Powercor - IR015 - ICT, CER and cyber security - 20250428 – public, page 20

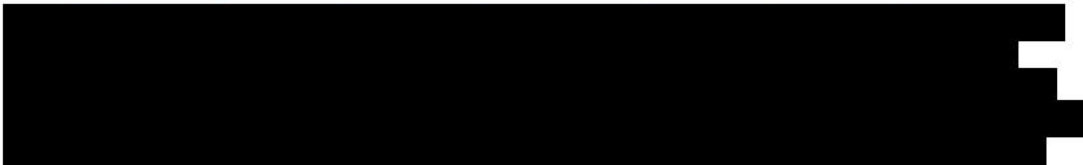
¹¹ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 12

- Option 3: Achieve market leading cyber security maturity – this is based on achieving 100% of the SP-3 (V2) practices, which is the current maximum under the AESCSF.
58. It is reasonable for CPU to consider 'Option 0' (do nothing, not presented above, but discussed in the business case) as not credible, because this would mean a worsening risk profile and which is unlikely to position the businesses to respond to likely higher SOCI Act obligations over the next RCP (e.g. a lift in minimum compliance to SP-2 (v2) or an equivalent).
59. Option 1 is rejected by CPU on reasonable grounds: *'An absence of uplift and progress in developing cyber security capabilities would likely result in an increased likelihood and greater consequence of a successful cyber attack...Maintaining a SP1+ level of cyber maturity will be insufficient.'*¹²
60. Option 3 is also reasonably rejected by CPU on the basis that *'Undertaking the additional practices related to SP3 will deliver minor improvements in risk reduction relative to option two, but overall, we estimate that our level of risk will remain substantively unchanged from the 2021–26 regulatory period.'*¹³ Suffice to say, we see no material advantage from the incremental cost CPU quotes (\$5.6 million, \$2024).
61. For Option 2, CPU describes in reasonable detail the 11 'focus areas' that it will invest in to build capability across the next RCP, noting that *'several initiatives focus specifically on protecting against new risks associated with CER devices.'*¹⁴ We sought more information to enable us to understand the proposed initiatives within each focus area. We are satisfied on the basis of the response¹⁵ that CPU has pursued an appropriately robust process to identify and prioritise the controls.
62. From the cost spreadsheet provided, discussed in more detail below, we can observe the apportionment of the proposed capex and opex across the 11 focus areas. From the benefits spreadsheet, also discussed further below, we can see the quantification of the qualitative benefits.
63. CPU does not explicitly map the initiatives to the AESCSF domains, which would have been useful, however it does provide a qualitative map of 'focus areas' against six sources of cyber security threat. This is helpful in comparing options and sense-checking the emphases of Option 2.
64. Option 2 will, according to CPU's risk-based analysis, result in 100% of SP-2 (V2) practices and 80% of SP-3 (V2) practices. This is commensurate with other risk-based analyses that we have seen:¹⁶

'Our proposed program of work will enable us to identify, protect, detect, respond and recover from cyber threats, and is based on people, processes and technology... While the AESCSF version 2.0 is useful to help benchmark maturity and minimum mandated compliance, a risk managed approach specific to our own network's risks and priorities is the key approach considered for our 2026–31 program.'

65. Overall, we consider Option 2 to be the prudent choice.

CPU proposes a significant uplift to its cyber team as part of its preferred option

66. 

¹² PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 13

¹³ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 21

¹⁴ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 16

¹⁵ Powercor - IR015 - Q12 - cyber security gap analysis - confidential

¹⁶ PAL BUS 7.02 - Cyber security - Jan2025 – Confidential, page 23

[REDACTED]

[REDACTED]

Cost estimate build-up is presented in adequate detail

68. CPU has presented a cost spreadsheet for the three options. Referring to the expenditure profile for Option 2 in Figure 2.4 and the data in the spreadsheet we note that:

- The capex and opex profiles are as we would expect – that is capex to establish new and enhanced controls tapers off progressively whilst opex (recurrent and non-recurrent) is forecast to build up progressively
- The opex step change is comprised of incremental staff, contractors, and licence/charges for new or upgraded systems and applications; the increased staff cost alone is over 50% of the step-change, with recurrent contractors representing the smallest contribution

- [REDACTED]

[REDACTED]

[REDACTED]

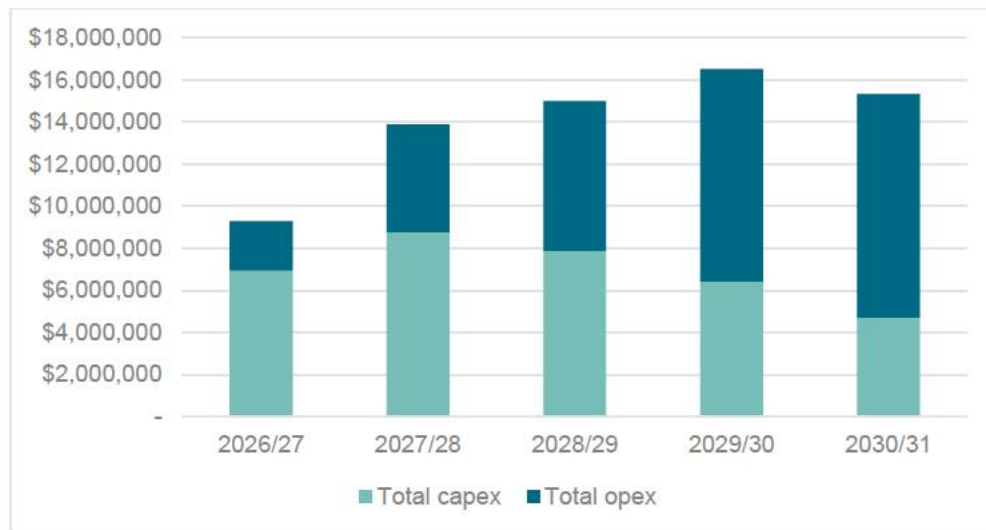
[REDACTED]

[REDACTED]

[REDACTED]

69. Based on the information provided and given the stage of the project lifecycle, we consider that CPU's cost estimate is reasonable.

Figure 2.4: CP + PAL + UE cyber security expenditure forecast – Option 2 (\$2024)

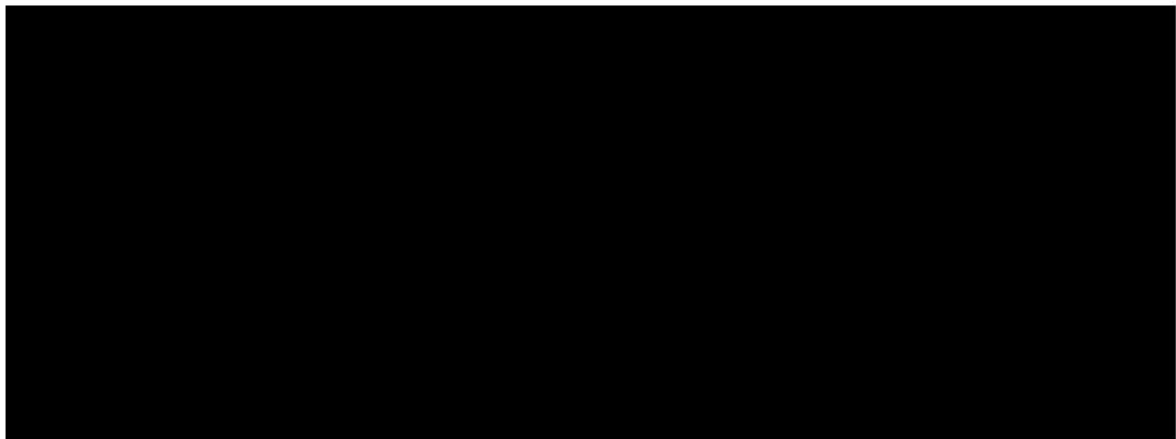


Source: PAL MOD 7.03 - Cyber security cost - Jan2025 – Confidential

Benefit analysis is presented in detail and whilst it likely overstates the benefit the NPV is still likely to be strongly positive

70. CPU has developed a detailed risk-cost analysis¹⁷ with transparent input values and the bases for the assumptions. The risk assessment and monetisation methodology are both consistent with other NSPs that have undertaken CBA analysis for their respective cyber security investment programs.
71. Our understanding is that CPU's proposed investments are to enhance cyber security capability to ensure compliance with its SOCI Act obligations and to *maintain* the risk level from the start of the next RCP to the end. It is commensurate with good industry practice to provide a CBA model.
72. [REDACTED]
73. [REDACTED]
74. However, even a moderation of this value and the Option 2 and 3 inputs would still lead to a strongly positive NPV for Options 2 and 3.

¹⁷ For example, PAL MOD 7.04 - Cyber security risk - Jan2025 - Confidential



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

2.5.1 Summary of our findings

75. We consider that CPU's proposed capex and opex step change are reasonable.

CPU's current period expenditure has responded to escalating risk but remains 'High' at the start of the next RCP

76. CPU has demonstrated a good understanding of the cyber security threat landscape, its increasing attack surface, and its compliance obligations under the SOCI Act.
77. In terms of its SOCI obligations, it has satisfied the requirement to achieve and sustain SP-1 practices in accordance with the AESCSF, noting that a higher Security Profile is formally recognised only when all the practices/anti-patterns are established and supported on an ongoing basis.
78. Recognising the increasing cyber risk level since the start of the current RCP, CPU has invested significantly in building its cyber security capabilities. Despite this investment, we consider that the risk rating is reasonably classified by CPU as 'High' at the start of the next RCP primarily because of the potential consequences arising from a serious successful attack.

CPU proposed significant further uplift in cyber maturity in the next RCP is appropriate and is targeted at the highest risk-mitigating areas

79. CPU's strategy of undertaking a risk-based approach to determining what controls are required is appropriate and leads to:
- Maintaining the cyber security risk level across the next RCP despite the increasing external threats, and
 - As measured against the AESCSF, 100% of SP-2 (V2) and about 80% of SP-3 (V2) practices being implemented.

80. 

81. CPU has presented a cost-benefit analysis which adequately demonstrates that the investment is likely to generate a positive NPV.

2.5.2 Implications for proposed capex and opex step change allowances

82. We consider that the capex proposed for each CPU business is reasonable and that the proposed opex step changes are reasonable estimates of incremental opex that each business will need to incur.

APPENDIX A CYBER SECURITY BACKGROUND AND CONTEXT INFORMATION

A.1 Cyber security threat in Australia

Increasing threat level is reported by the ACSC

83. The Australian Signal Directorate's (ASD) Australian Cyber Security Centre ('ACSC') monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2023-24) it states that: *'In FY2023-24, ASD received over 36,700 calls to its Australian Cyber Security Hotline, an increase of 12% from the previous financial year. ASD also responded to over 1,100 cyber security incidents, highlighting the continued exploitation of Australian systems and ongoing threat to our critical networks.'*¹⁸

There is an increasing cyber threat against critical infrastructure

84. State actors are focussed on critical infrastructure worldwide
85. The Australian Signals Directorate (ASD) states:
- 'State-sponsored cyber actors persistently target Australian governments, critical infrastructure and businesses using evolving tradecraft. These actors conduct cyber operations in pursuit of state goals, including for espionage, in exerting malign influence, interference and coercion, and in seeking to pre-position on networks for disruptive cyber attacks.'*¹⁹
86. Australian critical infrastructure has been targeted:²⁰
- 'Critical infrastructure networks are an attractive target due to the sensitive data they hold and the widespread disruption that a cyber security incident can cause on those networks. In FY2023-24, over 11% of cyber security incidents ASD responded to related to critical infrastructure. Compromise could lead to the disruption of critical services, affecting the economy and lives of everyday Australians.'*
87. The 2024 Report further states that: *'Operational technology systems are increasingly interconnected and can have vulnerabilities that make them an easier cyber target. Secure information and communications technology and operational technology systems are necessary to protect Australia's critical services.'*²¹
88. The ASD advises that: *'Critical infrastructure organisations should adopt a stance of 'when' not 'if' a cyber security incident will occur.'*²²

A.2 Critical Infrastructure Regulation

A.2.1 Amendments to the SOCI Act

¹⁸ ASD Cyber Threat Report 2023-24. Executive Summary

¹⁹ ASD Cyber Threat Report 2023-24. Executive Summary

²⁰ ASD Cyber Threat Report 2023-24. Executive Summary

²¹ ASD Cyber Threat Report 2023-24. Chapter 2

²² ASD Cyber Threat Report 2023-24. Chapter 2

89. The Security of Critical Infrastructure Act 2018 (SOCI Act) places obligations on specific entities in the electricity industry. It was amended in 2021 and 2022 to more appropriately capture those assets that are critical to Australia's defence, national security, economy and social stability. It was further amended in 2024 by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (ERP Act) in response to significant incidents impacting critical infrastructure. The objectives of the amendments were to lift existing obligations for responsible entities under the Act and to enhance the government's ability to manage the consequences of all hazardous incidents on critical infrastructure assets.²³ Figure A.1 summarises the relevant obligations.

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

- 1 **SOCI Act Subsection 12(F): Obligation to notify data service providers** – Entities must notify external data service providers if they are storing or processing **business critical data**. This ensures that companies that are handling sensitive data for critical infrastructure assets are aware that they may themselves also have obligations under the Act and that they treat the security of the data appropriately.
- 2 **SOCI Act Part 2: Register of Critical Infrastructure Assets** – Entities must register certain information related to critical infrastructure assets with the Cyber and Infrastructure Security Centre. Registration provides the Centre with a comprehensive understanding of the ownership and operational arrangements of critical infrastructure across the Australian economy. This helps the Government to better identify and respond to security risks.
- 3 **SOCI Act Part 2A: Risk Management Program** – Entities must have and comply with a Risk Management Program for their critical infrastructure assets. This will ensure responsible entities have a comprehensive understanding of the threat environment, and develop processes and procedures to effectively respond to the material risk of any hazard impacting their asset. This includes submitting an Annual Report 90 days after the end of the financial year.
- 4 **SOCI Act Part 2B: Mandatory Cyber Incident Reporting** – Entities must report cyber security incidents that have a **significant** or **relevant** impact on their asset. This information will support Government to develop an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance to working with industry to uplift broader security standards.
- 5 **SOCI Act Part 2C: Enhanced Cyber Security Obligations (ECSO)** – The Minister for Home Affairs, after consultation with the responsible entity and others, may declare an asset to be a 'System of National Significance'. These assets are those that are most crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors. If declared to be a system of national significance, the responsible entity may be notified that they are subject to four additional obligations focused on cyber preparedness and resilience.

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

90. [REDACTED]

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

91. 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.²⁵ 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.²⁶
92. The AESCSF Framework Core published by AEMO is one of the five documents referred to in the CIRMP instrument and the condition that is required to be met is SP-1. Therefore SP-1 is the legislative obligation that Network Service Providers (NSPs) must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.
93. Equally, the *Essential Eight Maturity Model* (EEMM) published by the Australian Signals Directorate is another referenced framework and the condition if it is adopted by an NSP is meeting Maturity Indicator Level one (MIL-1). Therefore MIL-1 is the legislative obligation to which NSPs must comply with if the NSP is defined as a responsible entity and the NSP selects the EEMM as its cyber security framework.

Privacy Act amendments 2022²⁷

94. The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill) amends the Privacy Act 1988 to expand the Australian Information Commissioner's enforcement and information sharing powers, and to increase penalties for serious or repeated interferences with privacy.
95. 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.
96. Within the Explanatory Memorandum to the Bill, it is stated that *'[t]his maximum penalty was introduced through the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022, which implemented the recommendation in the July 2019 report of the Australian Competition and Consumer Commission's Digital Platforms Inquiry to ensure penalties sufficiently deterred breaches of privacy, particularly for large digital platforms, and that individuals are adequately protected.'*²⁸
97. The Privacy and Other Legislation Amendment Bill 2024 (Cth) received Royal Assent and is now referred to as the Privacy and Other Legislation Amendment Act 2024 (Cth) (Amendment Act).

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

²⁴ <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf>

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

²⁶ 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).

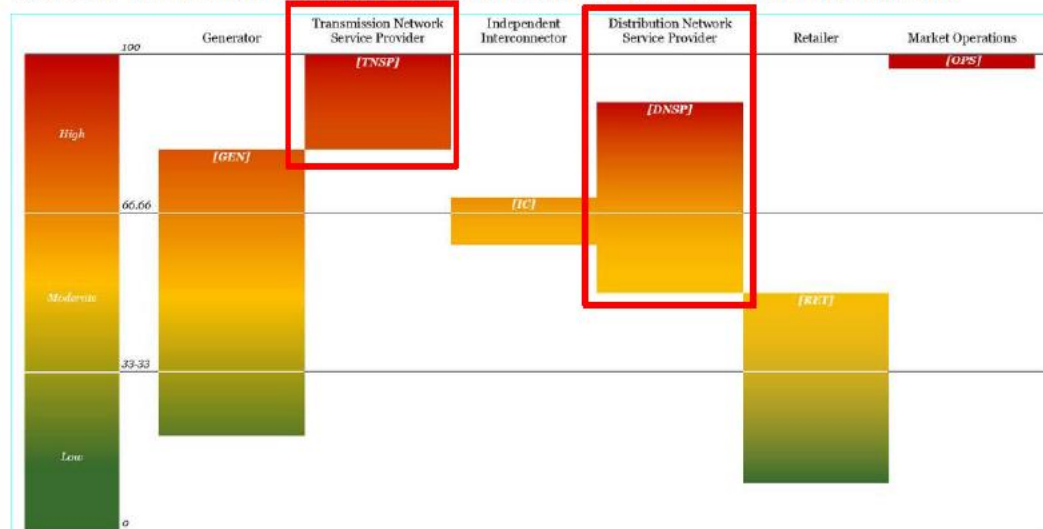
²⁷ https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6940.

²⁸ Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 EXPLANATORY MEMORANDUM, in reference to Section 13G – civil penalties (para 81).

A.3.1 AESCSF V1

98. 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.²⁹ The AESCSF Version 1 (V1) is divided into 11 domains, ten C2M2³⁰ 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 2021.³¹ AESCSF V1 encompasses the 2018 and subsequent iterations up to and including the 2022 revision.
99. 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.
100. The E-CAT allows assessment of the relative criticality of entities participating in the electricity and other energy sectors. The diagram below represents the criticality banding for the electricity sub-sector only, with DNSP criticality rating ranging between the High and Medium bands.

Figure A.2: AESCSF E-CAT CRITICALITY BANDS FOR ELECTRICITY SECTOR – DNSPS HIGHLIGHTED



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

A.3.2 AESCSF Version 2 (V2)

101. In December 2022, Energy Ministers endorsed AESCSF V2, providing guidance about the continued role of the program to support energy sector cyber uplift and increasing cyber security requirements for the energy sector in line with escalating and evolving cyber threats.
102. AESCSF V2 was released in 2023. The update to AESCSF v2 has resulted in an additional 72 practices (i.e. 20% additional practices). A summary of the difference between AESCSF V1 and V2 is summarised in v2.1 and AESCSF v2 is provided in Table A.1: AEMO has stated previously that '[t]he CAT should be treated as general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.'³²

²⁹ AEMO, AESCSF Framework and Resources, AEMO website.

³⁰ United States Department of Energy Cyber Security Capability Maturity Model.

³¹ AEMO AESCSF Framework Overview – 2022 Program. Page 1.

³² AEMO AESCSF Framework Overview – 2022 Program. Page 3.

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

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

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

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

APPENDIX B RELEVANT AER GUIDELINES FOR ASSESSMENT OF ICT EXPENDITURE

B.1 AER Guidelines for non-network ICT assessment

B.1.1 Assessment of non-network ICT capex

104. The scope of our assessment includes ex ante cyber security and ADMS capex, which are categorised as non-network ICT.
105. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to CPU's proposed cyber security capex. The proposed expenditure is also 'non-recurrent'.
106. 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:³³

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

107. 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.³⁴ We consider that such investments should be justified on the basis of a business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate 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.³⁵

Complying with new / altered regulatory obligations / requirements

108. 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.³⁶

New or expanded ICT capability, functions and services

109. 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.

³³ 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.

³⁴ The only exception will be where the business can demonstrate that any unquantified/intangible benefits of an option can support the decision to not choose the highest NPV option.

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

³⁶ AER, Non-network ICT capex assessment approach, November 2019. Page 11.

For each subcategory of non-recurrent expenditure, we note that there may be cases where the highest NPV option is not chosen. In these cases, where either the chosen option achieves benefits that are qualitative or intangible, we would expect evidence to support the qualitative assumptions. We consider the evidence provided must be commensurate with the cost difference between the chosen and highest NPV option.

We also note that where non-recurrent projects either lead to or become recurrent expenditures in the future, this needs to be identified in the supporting business case and accounted for in any financial analysis undertaken to support the investment.³⁷

B.1.2 Assessment of opex step changes

110. Our scope includes assessment of Jemena's proposed cyber security opex step changes. Section 2.2 of the AER's Expenditure Forecast Assessment Guideline for Electricity Distribution outlines its general approach for assessing opex step changes and which we have followed. In summary:
- The AER separately assesses the 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.³⁸

³⁷ AER, Non-network ICT capex assessment approach, November 2019. Page 12.

³⁸ AER, Expenditure Forecast Assessment Guideline for Electricity Distribution. Page 11.