EMCa

energy market consulting associates

Jemena 2026 - 2031 Regulatory Proposal

REVIEW OF PROPOSED EXPENDITURE ON CYBER SECURITY

[redacted]

Report prepared for:

AUSTRALIAN ENERGY REGULATOR (AER)

August 2025

Preface

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be allowed for the prescribed distribution services of Jemena 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 Jemena. 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 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 Jemena's regulatory submission or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell
Managing Director
psell@emca.com.au

Prepared by
Mark de Laeter, Paul Sell and Eddie Syadan

Date saved
26/09/2025 11:24 AM

Version
Final v3

Energy Market Consulting associates
ABN 75 102 418 020

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

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

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

Term	Definition
[redacted]	[redacted]
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
[redacted]	[redacted]
AMI	Advanced Metering Infrastructure
ASD	Australian Signals Directorate
C2M2	Cyber Security Maturity Model
CASB	Cloud Access Security Broker
Capex	Capital expenditure
CBA	Cost Benefit Analysis
CBAM	Cost Benefit Analysis Model
CER	Consumer Energy Resources
Current RCP	2022-2026 RCP
DNSP	Distribution Network Service Provider
E-CAT	Electricity Criticality Assessment Tool
[redacted]	[redacted]
EEMM	Essential Eight Maturity Model
FTE	Full Time Equivalent
GIP	Good Industry Practice
IAM	Identity and Access Management
ICT	Information Communication Technology
IT	Information Technology
JEN	Jemena Electricity Distribution Network
MIL-1	Meeting Maturity Indicator Level One
NER	National Electricity Rules
Next RCP	2027-2031 RCP
NIST	National Institute of Science and Technology
NPV	Net Present Value
NSP	Network Service Provider's
Opex	Operating expenditure
OT	Operational Technology

Term	Definition
[redacted]	[redacted]
[redacted]	[redacted]
Propex	Project opex
RCP	Regulatory Control Period
RIN	Regulatory Information Notice
RP	Regulatory Proposal
SCADA	Supervisory Control and Data Acquisition
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Totex	Total expenditure
ZTA	Zero Trust Architecture

1 INTRODUCTION

The AER has asked us to review and provide advice on aspects of Jemena's 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 Jemena's cyber security program is separate from our other reports for the AER pertaining to Jemena's forecast expenditure for ICT and CER.

Our review is based on information that Jemena 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 Jemena has proposed in its regulatory proposal (RP) for next RCP.
2. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed expenditures allowance as an input to its Draft Determination on Jemena's revenue requirements for the next RCP.

1.2 Scope of requested work

3. Our scope of work, covered by this report, is as defined by the AER, covers ex-ante capex related to ICT cyber security and opex step changes.
4. Other aspect of Jemena's expenditure, including repex, augex, other ICT capex, CER and opex step changes related to the hazard tree reduction, ICT and CER, are covered in two separate reports.

1.3 Our review approach

1.3.1 Approach overview

5. In conducting this review, we first reviewed the RP documents that Jemena has submitted to the AER. This includes a range of appendices and attachments to Jemena's RP and certain Excel models which are relevant to our scope.
6. We next collated several information requests. The AER combined these with information request topics from its own review and sent these to Jemena.
7. In conjunction with AER staff, our review team met with Jemena at its offices in late March 2025. Jemena presented to our team on the scoped topics, and we had the opportunity to engage with Jemena to consolidate our understanding of its proposal.
8. Jemena provided the AER with responses to information requests and, where they added relevant information, these responses are referenced within this review.
9. We have subjected the findings presented in this report to our peer review and Quality Assurance processes and we presented summaries of our findings to the AER prior to finalising this report.

1.3.2 Conformance with NER requirements

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

Capex Objectives and Criteria

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

12. The NER's capital expenditure criteria and capital expenditure objectives are reproduced in Figure 1.1 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

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

Figure 1.3: 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 and opex criteria and objectives in our assessment

14. 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 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*' 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 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, and
- 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.

15. 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.

1.3.3 Technical review

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

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

18. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what Jemena 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 Jemena's regulatory submission 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

19. In the next section, we have presented:

- An overview of the proposed expenditure and a summary of Jemena'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.

20. We also provide the following appendices:

- Appendix A in which we provide Cyber security background, and
- Appendix B for relevant AER Guidelines.

21. We have taken as read the considerable volume of material and analysis that Jemena 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

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

23. Except where specifically noted, this report was prepared based on information provided by AER staff prior to 1 June 2025 and any information provided subsequent to this time may not have been taken into account.

1.4.3 Presentation of expenditure amounts

24. 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.

25. 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

Jemena Group proposes $8.4 million expenditure comprising propex (project-related opex to establish enhanced Zero Trust capabilities) and an opex step change of $2.3 million. No capex is required in the next RCP.

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

Jemena Group has established a significant cyber security capability in the current RCP which, indirectly, its customers have benefitted from through both economies of scale and costs.

We find that Jemena Group'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.

Jemena Group proposes an uplift in in its cyber security capability at a reasonable cost.

2.1 Introduction

26. Jemena has provided an Investment Brief to justify an uplift in its cyber security capability over the next RCP in response to increasing cyber security threats.
27. Jemena is apportioned a 35.1% allocation of Jemena Group costs, given that cyber security is managed at the 'enterprise level'. Where relevant, we distinguish between the Jemena Group capabilities, analyses, initiatives and costs, and Jemena the DNSP.

2.2 Background and context

28. In Appendix A 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.
29. In undertaking our assessment, we take account of the following factors.

Increasing threat landscape and attack surface mean cyber risk is increasing

30. 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.
31. In our assessment we have sought to understand how Jemena has incorporated the increasing threat landscape and attack surface issues into its risk analysis and, ultimately into its option selection and proposed expenditure profile.

[redacted]

32. [redacted]

[redacted]

33. [redacted]

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

35. We have assessed how Jemena 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.

36. We have also considered whether Jemena has identified any other relevant obligations.

37. [redacted]

2.3 Overview and summary of Jemena's proposed expenditure

2.3.1 What Jemena has proposed in its RP

38. Jemena proposes to maintain its existing cyber security controls and invest in additional security capabilities over the course of the next RCP at a cost of $8.4 million opex. In Table 2.1 we show Jemena's proposed annual recurrent step-opex and the non-recurrent 'project opex' (propex) over the next RCP.

39. Jemena does not expect to require any capex.

[redacted]

Table 2.1: Jemena's proposed cyber security expenditure - $m, 2026)

Category	FY27	FY28	FY29	FY30	FY31	Total
[redacted]						
[redacted]						
[redacted]						
[redacted]						

Source: EMCa, from Jemena capex model (Att05-10M), opex model (Att06-03M), relevant CBAM and Jemena response to IR009 Q28

40. Jemena advises that the expenditure '*will embed cyber controls in step with technology advancement providing fit-for-purpose protection and response in line with cyber security threats, supporting JEN in the safe and reliable operation of the Jemena Electricity Network.*'[4]

41. Jemena further advises that the proposed program of works is an enterprise-wide initiative, with costs shared, leading to a 35.1% allocation to Jemena and which is reflected in the proposed expenditure above.

2.4 Assessment

2.4.1 Jemena's cyber security strategy and objectives

Jemena has adopted a risk-based approach to cyber security

42. Jemena advises that it uses a combination of the following to assess its cyber security risk:

[redacted]

43. These inputs inform its planning and implementation of appropriate controls and risk-reduction strategies.

2.4.2 Jemena's current state

Current capabilities

The Jemena Group has established a considerable cyber security capability in the current RCP

44. The whole-of-enterprise (aka Jemena Group) cost that it has incurred to date in the current RCP is a considerable $60.4 million, building over the period to $5 million in FY26.[5] The apportioned cost to Jemena and therefore to customers receiving SCS is considerably less at $21.2 million thanks to application of the Cost Allocation Methodology. No further capex is required in the next RCP, however Jemena proposes continuing to spend $2.4m p.a. (the 2025 base year recurrent opex) going forward on maintaining current services, plus propex and an opex step change for enhanced capabilities, which we assess below.

Jemena has familiar controls which support the self-assessment of its current capability

45. Jemena's Investment Brief describes its current cyber security capabilities (aka key controls), which are summarised in Figure 2.1. It reports that it has '*a mature and stable*

[4] JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted], page 10

[5] Refer to Table 2.2, below

security function with ongoing recurrent investment that allows us to manage known risks' because of its investment in staff and technology.[6]

46. In our view, whilst not mapped in the information provided to the AESCSF domains, the controls are familiar and consistent with good industry practice.

Figure 2.1: Jemena's current key cyber security controls

Source: JEN EMCa AER workshop 280325 - ICT and Cyber, slide 23

Jemena's most recent AESCSF assessment was in 2023

47. We asked Jemena to provide its current AESCSF maturity assessment results to help us understand both its then current enterprise cyber maturity level and its outlook through to the end of the current RCP.

48. Jemena provided its AESCSF Benchmarking dashboard March 2023 report which shows that at this time, it had achieved: [7]

[redacted]

49. From the report this is demonstrably a relatively strong cyber security profile among its peers and is certainly sufficient to confirm Jemena's statement in its assessment that it has '*an appropriate level of maturity…'*[8] Whilst controls to achieve SP practices vary in complexity and cost, we would expect from its early 2023 benchmark that the gaps to manage emerging risks are not large.

Jemena Group has a large in-house cyber security team in place

50. We asked Jemena to provide its Jemena Group cyber security team structure, head count, and cost and to also explain (i) what changes, if any, were expected over the duration of the next RCP, and (ii) what arrangements were in place to supplement the intern team with external advice (and for what purpose).

51. The team structure covering all of the Jemena Group is shown in Table 2.3, having grown from 13 FTEs in 2020, to 18 in 2021, and to 26 in 2025. Jemena also identified that it receives relatively modest external support for [redacted] and [redacted].[9]

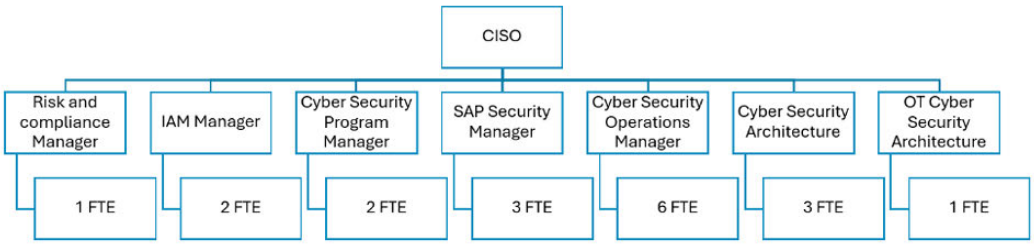
6 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted], page 5

7 Jemena's response to IR009 question 41, noting that precise practice counts were not provided

8 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected [redacted] page 4

9 JEN – RIN - Support -Cybersecurity Program - CBA Model - 20250415 – Confidential, tab Enterprise Cost build-up

Figure 2.2: Jemena Group's cyber security team



Source: Jemena response to IR009, question 39

Jemena's cyber security strategy is aligned with GIP

52. Jemena has adopted a strategy that is now common in the industry of undertaking a risk-based analysis and to invest in maintaining current levels of risk across the three risk scenarios it has focussed on:

- Damage or compromise to critical components leading to compromised network availability, reliability, integrity of the network, and confidentiality of data
- Damage or compromise to AMI meters resulting in a mass disconnection of customers, and
- Interference with critical IT/OT system (incl SCADA) leading to compromised availability, reliability and integrity of the network.

53. These risk scenarios are commonly applied in the industry as part of qualitative and/or quantitative risk analyses.

54. Jemena is not targeting a particular AESCSF maturity level. Our understanding is that instead it uses the AESCSF and the NIST framework and other inputs to access capability gaps, risks, and the appropriate controls.

2.4.3 Problem definition and risk assessment

55. Jemena notes that

> *'Cyber security risk is the most probable harm that could cause the widest possible impact on the safe and reliable delivery of electricity to our customers… and that '[t]o meet customer expectations for safe and reliable electricity supply [it] must continue to invest in capability to identify, protect, detect, respond and recover from cyberattacks.'*[10]

Increased cyber threat and compliance obligations

56. In its Investment Brief and its Technology Plan, Jemena has adequately identified (i) its legislative obligations and the increasing threat landscape (referring for example to the ASD's annual cyber threat report), and (iii) its own increasing attack surface area:[11]

> *'The autonomous nature of smart devices, their interdependency with ICT systems and their growing reliance on 3rd parties through digitisation are creating blind spots and increasing the potential for ICT exposure and exploitation by cyberattacks.'*

57. We are satisfied that, like its peer NSPs, all operating critical infrastructure, Jemena faces considerable and increasing cyber security threats from increasingly sophisticated actors and with increasing complexity.

Current period expenditure

58. Jemena advises that in the current period it expects to spend $8.6 million capex to implement existing on-premises capability and a combined $12.6 million opex to establish

[10] JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted] pages 6, 7

[11] JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted] page 7

and operate its cyber security operations, including team structure, licensing and project-related opex. The current period totex is $21.2 million as shown in Table 2.2. At 35.1% allocation to Jemena SCS, the enterprise cost we assume to be $60.4 million across the whole of business, $35.9 million of which is opex.

Table 2.2: Jemena electricity (JEN) share of cyber security expenditure in the current period - $m, real 2026

	FY22	FY23	FY24	FY25(E)	FY26(E)	TOTAL
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Source: IR009 – Question 25 EMCA Request.xls

Jemena's risk analysis

Jemena's risk analysis is qualitative but is largely consistent with assessment of its peers

59. [redacted] peer NSPs, all operating critical infrastructure, Jemena faces considerable and increasing cyber security threat which, also like its peers, requires consideration of the adequacy of its current controls.

12 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – SOCI, page 7

Jemena's gap analysis identified additional security capabilities required

61. Jemena highlights the rise in cyber actors' sophistication and threats to IT systems, OT systems and devices, customer IoT-connected appliances, and renewable energy devices integrated into the grid:

62. Jemena's gap analysis in this context led it to basing its forecast on implementing three zero trust-related solutions:

63. It is somewhat surprising that with Jemena's current level of cyber security maturity it requires further significant investment in Zero Trust-related capability notwithstanding that (i) these capabilities are evolving,[17] and (ii) recognising the additional emphasis on cyber security architecture and risk management (enterprise and third-party) in

13 'current' refers to the current controls and 'current' consequences, likelihood, and risk ratings; these are Jemena's assessment for the end of the current RCP with the current controls in place

64. Nonetheless, the Zero Trust[18] principle of 'never trust, always verify' and the associated components of Zero Trust Architecture (ZTA), Zero Trust Policy and Zero Trust Culture are all fundamental to good cyber security practice. Jemena's proposed implementation of [redacted] are each fundamental to enabling ZTA.

2.4.4 Jemena's cyber security options analysis

Jemena considered only two options

65. Jemena's Investment Brief includes analysis of the following options after rejecting a third option (delaying the project by a year):

1. Maintain the existing cyber security controls, and
2. Implement incremental fit-for-purpose cyber security controls to continue managing existing and emerging cyber threats (recommended).

Option 1 may not adequately address emerging cyber security threats

66. There is no incremental cost to this option because the expenditure is within the base year. Jemena concludes that this approach will:[19]

- Progressively increase the likelihood of a successful cyber-attack that impacts the safe supply of electricity to its customers as the gap widens between control effectiveness and emerging and evolving threats, and
- [redacted]

67. In our view, despite Jemena's relatively high level of cyber security maturity it has identified gaps in its capability that if not addressed will expose the Jemena Group to an increasing likelihood of a successful cyber-attack with network and customer implications. This would not be a prudent approach.

Option 2 is the likely to be the prudent investment

68. Whilst not evident from the description, Option 2 encompasses both maintaining the existing cyber security controls and adding the additional cyber security controls referred to above in our discussion of Jemena's capability gap analysis, namely:[20]

[redacted]

69. Reference is made in the business case to three other additional security capabilities which we assume are being implemented but at no incremental cost:

- An IoT security model
- A 'detect and protect' security model, and

---

18 Zero trust is a response to enterprise network trends that include remote users, bring your own device, and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource (NIST, Zero Trust Architecture, 2020 per NIST SP 800-207 and NIST SP 1800-35)

19 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted] page 8

20 Costs are derived from JEN – RIN - Support -Cybersecurity Program - CBA Model - 20250415 – Confidential, tab $2023 to $2024

21 [redacted]

- The cyber security 'shift left' model.

70. As discussed in our assessment of Jemena's gap analysis, we consider that the additional controls are consistent with the requirements of good cyber security practices.

71. Jemena has not quantified the benefits of its preferred Option 2, instead stating that the qualitative benefit is to '*reduce the risk rating from 'high' to 'significant' in the current threat environment.'*[22] We sought clarification from Jemena representatives at our onsite meeting about its cyber security objective. From the engagement, our understanding is that Jemena's program is intended to *maintain* the current risk level, which aligns with our interpretation of the intent (and risk maps) expressed in the Investment Brief, as discussed above.

72. Jemena has not presented a cost-benefit analysis for its proposed cyber-security investment. However, NSPs typically demonstrate that benefits exceed the costs of implementing the new/expanded cyber security capability through quantified cost-benefit analysis, in accordance with the AER's expectations for the sub-category of 'New or expanded ICT capability, functions and services',[23] although strictly the AER's requirement is based on capex assessment. Regardless, a cost-benefit analysis helps demonstrate the prudency of the selected option, among other things.

73. Jemena has chosen not to present a cost-benefit analysis to demonstrate the prudency of its selected option, instead relying on qualitative risk-benefit analysis for comparing the two identified options. This is not consistent with good industry practice.

74. Jemena also considered that deferring the program by a year ('Option 3') was not viable because it '*could expose JEN to significant cyber risks, leaving our systems outdated and vulnerable to security breaches…'* [24] In our view, the risk is somewhat overstated, mainly because of the significant cyber maturity that Jemena has achieved. Nonetheless, given that the financial benefit of deferral of the program by one year is at most $1.4 million reduced opex over the course of the next RCP, the benefit may well be outweighed by the risk-cost.[25] We therefore consider that deferral, in Jemena's case, is unlikely to be a prudent approach despite the lack of quantified analysis.

It is not clear what the outcome of Jemena's proposed investment in the next RCP will achieve in terms of the AESCSF

75. Whilst Jemena states it 'uses' the AESCSF to assess its cyber-security risk, it emphasised at the on-site meeting that Jemena Group is not targeting a certain level of AESCSF maturity. Instead, it reiterates that its proposed additional/enhanced controls in the next RCP are what its gap/risk analysis has led it to propose.

Cost estimates are likely to be reasonable, noting Jemena is allocated a proportion of the total cost

76. Jemena advises that:[26]

- The basis of the non-recurrent opex estimates is cloud-based, SaaS; internal and external labour using Hays rates and based on the security teams' estimate of the time required and from discussions with vendors, including [redacted] (who provided input on indicative pricing), and
- The basis of the recurrent step-opex estimates is licences for [redacted]; an existing license is in place for [redacted] and pricing accounts for incremental increases of the existing license. Since they involve new capability, it is reasonable to accept that these costs were not included in Jemena's base year opex.

22 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted] page 9

23 Refer to Appendix B

24 JEN – RIN – Support – ICT Investment Brief - Cyber Security Program – 20250131 – Protected – [redacted], page 8

25 We have undertaken and seen risk-cost analyses of various levels of cyber security investment and a range of *possible* successful breaches impacts would cause financial and other detriment far greater than $1.4 million.

26 JEN EMCa AER workshop 280325 - ICT and Cyber, slide 26

77. We consider that the resulting costs are likely to be reasonable based on the estimating methodologies.

2.5 Findings and implications

2.5.1 Summary of our findings

Jemena's cyber security capability, its assessment and proposed initiatives are reasonable

78. JEN has an advanced cyber capability already with a large in-house capability all included in the base year and will support the costs of maintaining current controls with no step-change.

79. Jemena has undertaken a gap analysis and explained its selection of corresponding additional controls to manage the risks to the extent that its risk profile from the start to finish of the next RCP is maintained (i.e. in the face of rising cyber threats and attack surface).

80. The proposed propex is justified based on Jemena's plan to introduce three new controls, which it has specified and adequately costed.

81. The step change opex is for new capabilities each related to enhanced ZTA [redacted] which in turn is now fundamental to good cyber security practice.

82. Jemena's options analysis is qualitative and would benefit from a quantitative CBA but we nevertheless consider that Jemena has selected the appropriate option (Option 2) and a reasonable cost.

2.5.2 Implications for proposed capex and opex step change allowances

83. We consider that Jemena's proposed cyber security propex is reasonable and that its proposed opex step change represents a reasonable estimate of its incremental expenditure.

APPENDIX A – CYBER SECURITY BACKGROUND AND CONTEXT INFORMATION

A.1 Cyber security threat in Australia

Increasing threat level is reported by the ACSC

84. 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.*'[27]

There is an increasing cyber threat against critical infrastructure

85. State actors are focussed on critical infrastructure worldwide

86. 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.*[28]

87. Australian critical infrastructure has been targeted:[29]

> *'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.'*

88. 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.*'[30]

89. The ASD advises that: '*Critical infrastructure organisations should adopt a stance of `when' not `if' a cyber security incident will occur.*'[31]

A.2 Critical Infrastructure Regulation

A.2.1 Amendments to the SOCI Act

27 ASD Cyber Threat Report 2023-24. Executive Summary

28 ASD Cyber Threat Report 2023-24. Executive Summary

29 ASD Cyber Threat Report 2023-24. Executive Summary

30 ASD Cyber Threat Report 2023-24. Chapter 2

31 ASD Cyber Threat Report 2023-24. Chapter 2

90. 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.[32] Figure A.1 summarises the relevant obligations.

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

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

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

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

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

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

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

91. [redacted]

32 [redacted]

[redacted]

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

92. 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.[34] 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.[35]

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

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

Privacy Act amendments 2022[36]

95. 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.

96. 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.

97. 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.* [37]

98. 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)

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

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

35 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).

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

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

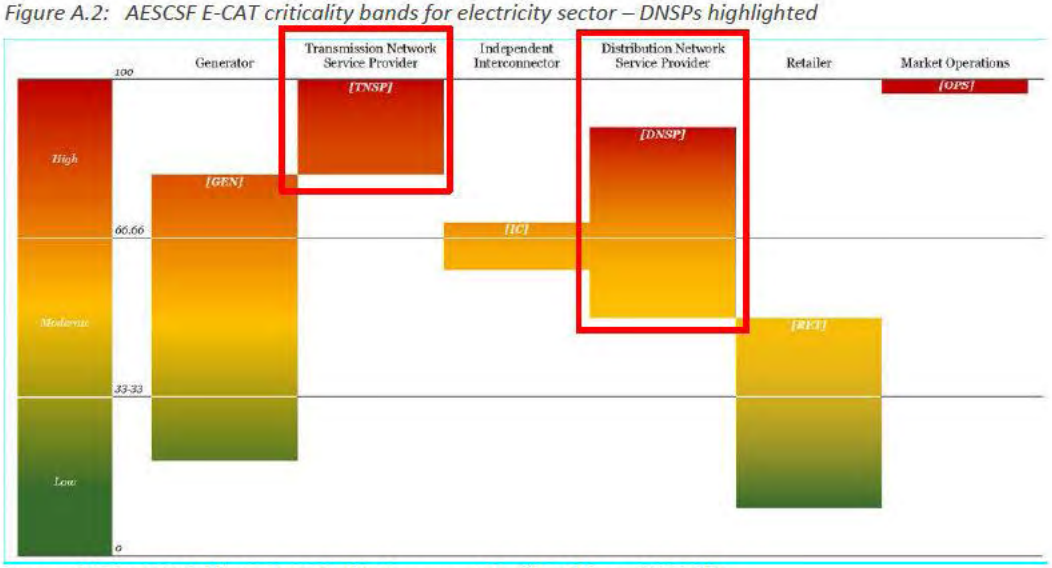
A.3.1 AESCSF V1

99. 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.[38] The AESCSF Version 1 (V1) is divided into 11 domains, ten C2M2[39] 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.[40] AESCSF V1 encompasses the 2018 and subsequent iterations up to and including the 2022 revision.

100. 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.

101. 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)

102. 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.

103. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting CIRMP minimum obligations), and a transition plan to 'sunset' AESCSF V1. AESCSF V2 was released in 2023. The update to AESCSF v2 has resulted in an additional 72 practices (i.e., 20% additional practices). A summary of the difference between AESCSF V1 and V2 is summarised in v2.1 and AESCSF v2 is provided 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.*'[41]

38 AEMO, AESCSF Framework and Resources, AEMO website.

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

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

41 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

104. 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 project expenditure

105. The scope of our assessment includes ex ante cyber security expenditure which is categorised as non-network ICT.

106. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to Jemena's proposed cyber security expenditure.

107. 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:[42]

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

108. 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.'* [43] *We consider that such investments should be justified on the basis of a business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency). The assessment methodology would also give regard to the past expenditure in this subcategory.*[44]

Complying with new / altered regulatory obligations / requirements

109. The AER states that:

> *It is likely that for such investments, the costs will exceed the measurable benefits and as such, the least cost option will likely be reasonably acceptable in regard to the NER expenditure criteria. Therefore the assessment of these expenditures is similar to subcategory one. Should there be options to achieve compliance through the use of external service provides [sic], the costs and merits of these should be compared.'*[45]

New or expanded ICT capability, functions and services

110. 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.*
>
> *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*

---

42 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.

43 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.

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

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

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.[46]

B.1.2 Assessment of opex step changes

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

- The AER separately assesses the prudency and efficiency of forecast cost increases or decreases from new regulatory obligations and capex/opex trade-offs;
- For capex/opex trade-off step changes, the emphasis is on establishing whether it is prudent and efficient to substitute opex for capex; and
- For step changes arising from new regulatory obligations, the emphasis is on:
  - whether there is a binding change in regulatory obligations that affects the efficient forecast opex and when the change occurred, and
  - what options were considered and whether the selected option is an efficient option.[47]

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

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