EMC[a]

energy market consulting associates

TasNetworks 2024 to 2029 Regulatory Proposal

REVIEW OF PROPOSED EXPENDITURE ON ICT CYBER SECURITY

Report prepared for:

AUSTRALIAN ENERGY REGULATOR

August 2023

Preface

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be allowed for the prescribed distribution services of TasNetworks from 1st July 2024 to 30th June 2029. The AER's determination is conducted in accordance with its responsibilities under the National Electricity Rules (NER).

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

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

Except where specifically noted, this report was prepared based on information provided to us prior to 1st July 2023 and any information provided subsequent to this time may not have been taken into account. Some numbers in this report may differ from those shown in TasNetworks' regulatory submission or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell
Managing Director
psell@emca.com.au

Prepared by
Mark de Laeter and Paul Sell with input from Cesare Tizi and Eddie Syadan

Date saved
27/09/2023 3:18 PM

Version
Final v4

Energy Market Consulting associates
ABN 75 102 418 020

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

Perth Office
Level 1, 2 Mill Street, Perth WA 6000
contact@emca.com.au
www.emca.com.au

TABLE OF CONTENTS

ABBREVIATIONS V

1 INTRODUCTION 1

1.1 Objective of this report 1

1.2 Scope of requested work 1

1.3 Our review approach 1

1.4 About this report 5

2 RELEVANT CONTEXT TO OUR ASSESSMENT 7

2.1 Cyber security threat in Australia 7

2.2 Critical infrastructure - changes to regulation 8

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

2.4 AER Guidelines for non-network ICT assessment 11

2.5 Implications for our assessment 13

3 TASNETWORKS' PROPOSED ICT CYBER SECURITY EXPENDITURE 15

3.1 Overview and summary of proposed expenditure 15

3.2 Summary of the basis for TasNetworks' proposed expenditure 16

4 OUR ASSESSMENT 18

4.1 TasNetworks' risk analysis 18

4.2 TasNetworks' cyber security-related objectives 19

4.3 TasNetworks' options analysis 20

4.4 TasNetworks' cost forecasting methodology 22

4.5 Other aspects 26

4.6 Our findings and implications 27

LIST OF TABLES

Table 3.1: TasNetworks' proposed non-recurrent ICT cyber security capex - $million, real FY2022 15

Table 3.2: TasNetworks' proposed ICT cyber security opex step changes - $, million real 2024 16

Table 4.1: EMCa proposed adjustment to TasNetworks proposed cyber security capex ($m) 28

Table 4.2: EMCa proposed adjustment to TasNetworks proposed cyber security opex step change ($m) 28

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: The cyber security problem 8
Figure 2.2: AESCSF E-CAT criticality bands for electricity sector – TNSPs and DNSPs highlighted 10
Figure 2.3: Relationship between SPs, participant criticality, practices/anti-patterns and MILs – per AESCSF V1 11
Figure 4.1: TasNetworks' cyber security journey 20
Figure 4.2: TasNetworks' proposed opex forecast over the next RCP ($m, real 2022) 24
Figure 4.3: Additional opex from additional FTEs ($m, real 2022) 25

ABBREVIATIONS

Term	Definition
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	The Australian Energy Sector Cyber Security Framework
CIRMP	Critical Infrastructure Risk Management Program
DNSP	Distribution Network Service Provider
ECSO	Enhanced Cyber Security Obligations
ICS	Information and communications Systems
ICT	Information and Communication Technology
IES	Inverter Energy System
IT	Information Technology
MIL	Maturity Indicator Level
NER	National Electricity Rules
RCP	Regulatory Control Period
NPV	Net Present Value
NSP	Network Service Provider's
opex	Operating expenditure
OT	Operational Technology
RP	Revenue Proposal
SLACI	Security Legislation Amendment Critical Infrastructure
SOCI	Security of Critical Infrastructure
SoNS	Systems of National Significance
SP	Security profile
TN	TasNetworks
TNSP	Transmission Network service Provider

1 INTRODUCTION

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

1.1 Objective of this report

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

1.2 Scope of requested work

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

1.3 Our review approach

1.3.1 Approach overview

6. In undertaking our review, we:
   - Completed a desktop review of the information provided to us by the AER followed by preparing requests for information to TasNetworks to help ensure that we correctly understood the methodology and assumptions that TasNetworks had applied in estimating its expenditure requirements;
   - Completed an assessment of relevant aspects of the expenditure forecast, including by taking into account the responses from TasNetworks to information requests; and
   - Documented our findings in this report.
7. We also provided feedback to AER staff on our preliminary findings in a teleconference, while drafting this report.
8. Our review considers the requirements of the National Electricity Rules (NER), specifically the capex and opex criteria and objectives, and the AER's expenditure assessment guideline.

[1] TasNetworks-Combined Proposal Attachment 6 - Capital expenditure-Jan-23 and TasNetworks-Combined Proposal Attachment 8 - Operating expenditure-Jan-23-Public

9. Where we find that TasNetworks' forecast expenditure is not reasonable in terms of the relevant requirements of the NER, we have identified the extent to which the issues we have found have resulted in a higher level of expenditure than what would be required of a prudent and efficient service provider.

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

1.3.2 Conformance with NER requirements

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

Capex Objectives and Criteria

12. The most relevant aspects of the NER in this regard are the 'capital expenditure criteria' and the 'capital expenditure objectives.' Specifically, the AER must accept the Network Service Provider's (NSP's) 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 capex criteria and capex objectives are reproduced in Figure 1.1 and Figure 1.2.

Figure 1.1: NER capital expenditure criteria

NER capital expenditure criteria

The AER must:

*(1) subject to subparagraph (c)(2), accept the forecast of required capital expenditure of a Distribution Network Service Provider that is included in a building block proposal if the AER is satisfied that the total of the forecast capital expenditure for the regulatory control period reasonably reflects each of the following (**the capital expenditure criteria**):*

(i) the efficient costs of achieving the capital expenditure objectives;

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

(iii) a realistic expectation of the demand forecast and cost inputs required to achieve the capital expenditure objectives.

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

Figure 1.2: NER capital expenditure objectives

NER capital expenditure objectives

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

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

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

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

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

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

to the relevant extent:

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

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

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

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

Opex Objectives and Criteria

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

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; and

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

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

Source: NER 6.5.6 (c) Forecast operating expenditure

Figure 1.4: NER operating expenditure objectives

NER operating expenditure objectives

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

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

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

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

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

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

to the relevant extent:

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

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

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

Source: NER 6.5.6 (a) Forecast operating expenditure

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

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

- Drawing on the wording of the first and second 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.

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.

1.3.3 Technical review

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

18. We have sought to assess TasNetworks' expenditure proposal based on TasNetworks' analysis and TasNetworks' 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 TasNetworks 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 TasNetworks 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 TasNetworks regulatory submission documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 About this report

1.4.1 Report structure

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

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

1.4.2 Information sources

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

22. Except where specifically noted, this report was prepared based on information provided to us AER staff prior to 1st July 2023 and any information provided subsequent to this time may not have been taken into account.

1.4.3 Presentation of expenditure amounts

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

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

2 RELEVANT CONTEXT TO OUR ASSESSMENT

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

2.1 Cyber security threat in Australia

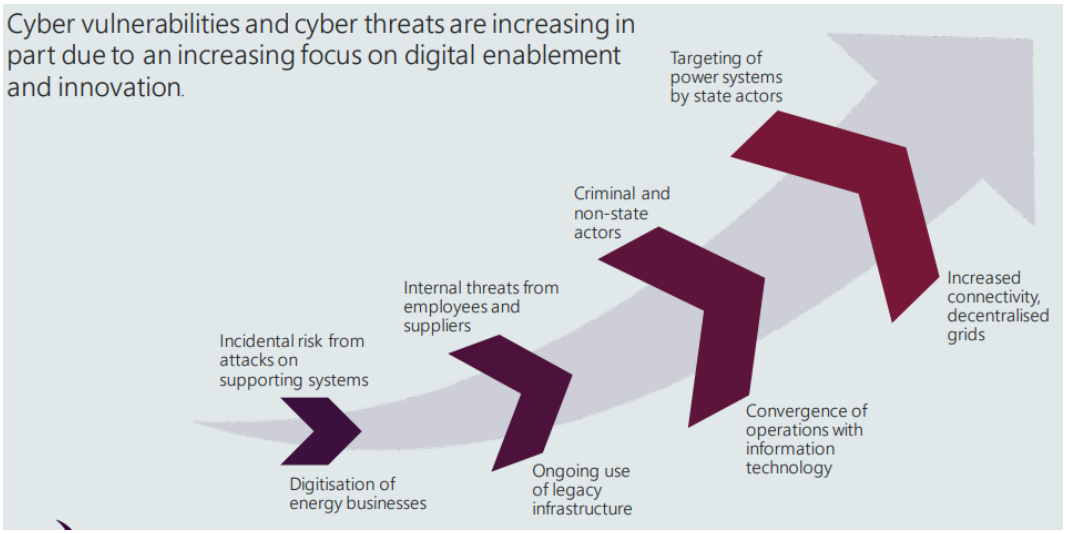
25. The Australian Cyber Security Centre ('ACSC') monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2021-22) it states that: *The ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous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

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

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

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

Figure 2.1: The cyber security problem



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

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

2.2 Critical infrastructure - changes to regulation

2.2.1 Amendments to the SOCI Act

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

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

31. The amendments were made because '*Australia is facing increasing cyber security threats to essential services, businesses and all levels of government.* [2] Electricity assets may be classed as critical infrastructure within the framework under the Act. The new 'Positive Security Obligations' that apply to certain sets of critical infrastructure assets are:

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

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

- A new obligation for responsible entities to create and maintain a critical infrastructure risk management program ('CIRMP') with the obligation commencing on 17 February 2023;[3] and

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

3 CISC Factsheet – Risk Management Program

- A new framework for enhanced cyber security obligations (ECSO) required for operators of systems of national significance (SoNS), Australia's most important critical infrastructure assets.[4]

33. The CIRMP is a written program which requires a responsible entity for a critical infrastructure asset to (i) to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, and so far as it is reasonably practicable to do so, (ii) minimise or eliminate any material risk of such a hazard occurring, and (iii) mitigate the relevant impact of such a hazard on the asset.[5]

34. The ECSO will vary between each SoNS, depending on the specific role and function of that asset, with the obligations including (i) developing cyber security incident response plans to prepare for a cyber security incident, (ii) undertaking cyber security exercises to build cyber preparedness, (iii) undertaking vulnerability assessments to identify vulnerabilities for remediation, and/or (iv) providing system information to develop and maintain a near real-time threat picture.[6]

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

35. Under the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023, a responsible entity must establish and maintain a process or system in the CIRMP to (a) comply with a framework contained in one of five documents referred to in the CIRMP, and (b) meet the corresponding condition for that document.[7] 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.[8]

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

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

2.2.3 Privacy Act amendments 2022[9]

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

39. The Bill increases the maximum penalty under section 13G of the Privacy Act for a body corporate to an amount not exceeding the greater of $50 million, three times the value of the benefit obtained, or, if the court cannot determine the value of the benefit, 30% of their adjusted turnover in the relevant period. The maximum penalty of $50 million is an increase from the pre-existing maximum of $2.22m.

---

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

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

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

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

8 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)

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

40. Within the Explanatory Memorandum to the Bill, it is stated that *'[b]y strengthening penalties, Australia will be signalling its expectations that businesses undertake robust privacy and security practices.'*[10]

2.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

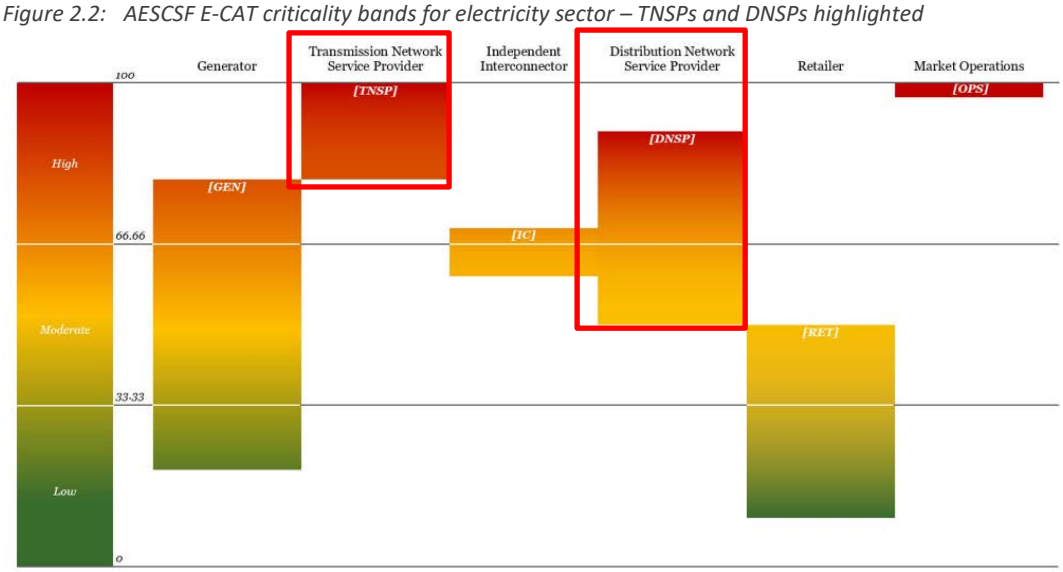
2.3.1 AESCSF V1

41. In response to the Finkel National Electricity Market Review recommendation 2.10, in 2018 the Australian Energy Market Operator (AEMO) collaborated with industry and government to develop the AESCSF. Among other markets, it covers Australia's electricity sector and is voluntary but has been adopted by NSPs.[11] The AESCSF is divided into 11 domains, ten C2M2[12] domains, and the Australian Privacy Management Domain. There were minor revisions to the AESCSF in 2019, 2021, and 2022, with no significant changes in version 2022 compared to version 2021.[13] AESCSF Version 1 (V1) encompasses the 2018 and subsequent iterations up to and including the 2022 revision.

42. 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.

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

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



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

44. The table in the figure below '*indicates which SP an organisation in the electricity sub-sector should achieve based on their criticality (as determined by the E-CAT)*.'[14] This may be construed as an obligation, however AEMO also states that '*[t]he CAT should be treated as*

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

11 AEMO, AESCSF Framework and Resources, AEMO website

12 United States Department of Energy Cyber Security Capability Maturity Model

13 AEMO AESCSF Framework Overview – 2022 Program, page 1

14 AEMO AESCSF Framework Overview – 2022 Program, page 9

general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.[15]

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

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

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

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

2.3.2 AESCSF Version 2 (V2)

46. 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.

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

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

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

2.4 AER Guidelines for non-network ICT assessment

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

15 AEMO AESCSF Framework Overview – 2022 Program, page 3

16 Asset, Change and Configuration Management

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

18 AEMO website, AESCSF Program

2.4.1 Assessment of non-recurrent ICT capex

50. The AER's 2019 Non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to TasNetworks' proposed cyber security capex.

51. The AER requires DNSPs to allocate their non-recurrent ICT expenditures into the three subcategories for which it applies different assessment approaches, as described below:[19]

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

52. The AER states that: *'Given that these expenditures are related to maintaining existing service, we note that it will not always be the case that the investment will have a positive NPV. As such, it is reasonable to choose the least negative NPV option from a range of feasible options including the counterfactual.[7] For such investments, we consider that they should be justified on the basis of the business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency). The assessment methodology would also give regard to the past expenditure in this subcategory.'*

Complying with new / altered regulatory obligations / requirements

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

New or expanded ICT capability, functions and services

54. 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.*

55. *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.*

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

2.4.2 Assessment of opex step changes

57. Section 2.2 of the AER's Expenditure Forecast Assessment Guideline for Electricity Distribution outlines its general approach for assessing opex step changes and which we have followed. In summary:[20]

- The AER separately assesses the prudency and efficiency of forecast cost increases or decreases from new regulatory obligations and capex/opex trade-offs;
- For capex/opex trade-off step changes, the emphasis is on establishing whether it is prudent and efficient to substitute opex for capex; and
- For step changes arising from new regulatory obligations, the emphasis is on:

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

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

- whether there is a binding change in regulatory obligations that affects the efficient forecast opex and when the change occurred
- what options were considered and whether the selected option is an efficient option.

2.5 Implications for our assessment

Increasing threat landscape and attack surface mean cyber risk is increasing

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

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

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

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

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

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

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

63. We have assessed how TasNetworks 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.

64. We have also considered whether TasNetworks has identified any other relevant obligations.

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

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

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

67. Whilst AESCSF V2 has not been publicly released at the time of writing this report, we assume that because V2 was '…*developed in consultation with industry, governments and specialist agencies*…'[21] that TasNetworks was broadly aware of the likely increase in the hurdles (number of practices) to achieve each of the three MILs and three SPs compared to

[21] AEMO website, AESCSF Program

V1. Again, it is relevant to take into consideration TasNetworks' incorporation of future regulatory obligations where there is a reasonable evidenced understanding of what they will be, noting that it has the opportunity for applying to the AER for a pass through if new obligations occur after approval of its RP and which could not reasonably have been anticipated.

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

3 TASNETWORKS' PROPOSED ICT CYBER SECURITY EXPENDITURE

TasNetworks has proposed a capex allowance which we derive to be $8.99m in $2023/24 terms, together with an opex step change of $19.3m in $2023/24 terms. TasNetworks has attributed 80% of these costs to its transmission service and 20% to its distribution service.

3.1 Overview and summary of proposed expenditure

69. TasNetworks has proposed a cyber security-related capex of $8.1m in $2021/22 terms as shown in Table 3.1. We have converted this in our adjustment table (in section 4.6.2) to $8.90m in $2023/24, using information that TasNetworks provided in its IR#039 reconciliation workbook.

Table 3.1: TasNetworks' proposed non-recurrent ICT cyber security capex - $million, real FY2022

Initiative	2025	2026	2027	2028	2029	Total
[redacted]	0.0	0.0	0.0	0.2	0.2	**0.4**
[redacted]	0.2	0.0	0.0	0.0	0.2	**0.4**
[redacted]	0.3	0.3	0.0	0.0	0.0	**0.6**
[redacted]	0.0	0.2	0.2	0.2	0.0	**0.6**
[redacted]	0.1	0.1	0.1	0.0	0.0	**0.3**
[redacted]	0.1	0.0	0.0	0.0	0.0	**0.1**
[redacted]	0.0	0.1	0.1	0.0	0.0	**0.3**
[redacted]	0.0	0.0	0.3	0.3	0.3	**0.9**
[redacted]	0.0	0.4	0.4	0.0	0.0	**0.8**
[redacted]	0.5	0.6	0.6	0.6	0.0	**2.2**
[redacted]	0.0	0.0	0.0	0.1	0.0	**0.1**
[redacted]	0.3	0.0	0.0	0.0	0.0	**0.3**
[redacted]	0.2	0.2	0.2	0.2	0.2	**1.0**
[redacted]	0.0	0.0	0.1	0.1	0.0	**0.2**
TOTAL	**1.6**	**1.9**	**2.0**	**1.6**	**0.9**	**8.1**

Source: Table 19, TasNetworks Cyber Security Program of Work Investment Evaluation Summary – Oct 22 – Confidential

70. TasNetworks has proposed a cyber security-related opex step change of $19.3m in $2023/24, as shown in Table 3.2. Based on IR#039, we find that TasNetworks has derived this amount by converting a cost in $2021/22. However, we find that this has been converted incorrectly from an index from 2020.

71. In its IR#039 reconciliation, TasNetworks presents its opex step change as $16.2m in $2021-22, and which it derives by subtracting its base year value of $5.4m from its proposed overall opex of $21.6m. Applying its inflation indices, an opex step change of $16.2m in $2021-22 would convert to a step change amount of $17.8m (in $2023/24).

Table 3.2: TasNetworks' proposed ICT cyber security opex step changes - $, million real 2024

Step Change	2025	2026	2027	2028	2029	Total
Transmission cyber security	1.7	2.9	3.6	3.6	3.7	15.5
Distribution cyber security	0.4	0.7	0.9	0.9	0.9	3.9
Total	**2.1**	**3.7**	**4.4**	**4.6**	**4.6**	**19.3**

Source: TasNetworks – combined proposal Att. 8, Table 4 and Table 5

3.2 Summary of the basis for TasNetworks' proposed expenditure

3.2.1 Problem definition and risk assessment[22]

Increasing cyber threat landscape

72. TasNetworks presents background information concerning the escalating cyber security threat landscape:

> *'[t]he cyber security threat landscape is rapidly changing characterised by an increasing volume of successful attacks both nationally and across the globe…'* with challenges *'…exacerbated by an overwhelmingly complex technology stack…'* and which it attributes to *'…the evolution, growth and increasing dependency on technology…'* and *'… the challenges organisations face in finding and retaining skilled workers with specialist cyber security skills and qualifications.'*

73. In terms of the importance of TasNetworks transmission and distribution networks in the national context, it identifies the need to *'…uplift the security posture of* ICS/OT *technologies that were never designed, nor intended to be externally accessible'* given (i) the projected export of generating capacity to the mainland, and (ii) the supply chain risks from increasing interconnectivity of the grid.

Increasing cyber-attack surface

74. TasNetworks also highlights the increasing exposure of TasNetworks ICS/OT systems to external third and fourth parties presented from business process and technology integration (including PV, battery systems, and green hydrogen fuel). This has the effect of *'…increasing the attack surface that TasNetworks presents…'* with the next RCP presenting *'…a likely increased risk position for the organisation, requiring a security response.'*

TasNetworks' cyber security risks and risk rating

75. TasNetworks' position is that over the regulatory period 2024-2029, it will see an increase in its risk exposure and that the following cyber security risks require action:

1. *'Loss of control of the electricity network, leading to system black/market suspension condition.*
2. *Theft of sensitive information leading to financial loss and reputational damage.*
3. *Ransomware introduction leading to widespread disruption and loss of system availability in IT environment.*
4. *Ransomware introduction leading to widespread disruption and loss of system availability OT environment.*
5. *Ransomware introduction leading to theft and public exposure of sensitive information.*

[22] TasNetworks IES for Cyber Security Program of Work (R24), pages 3-8, 19, 35, 40

6. *Accidental loss of control of the electricity network, leading to system black/market suspension condition.*
7. *A network denial of service condition results in loss of telephony services and call centre availability.*
8. *Failure to adequately protect against cyber threats due to lack of comprehensive and trustworthy asset inventory and configuration management repository.'*

76. The overall risk rating is assessed by TasNetworks in [redacted]

3.2.2 TasNetworks' cyber security strategy and objectives

77. TasNetworks' cyber security strategy is to '*protect our critical assets – people, property and information – by establishing a contemporary enterprise-wide cyber security practice inclusive of human behaviour and technology-related threats and vulnerabilities.*'[23]

78. The TasNetworks Cyber Security Plan for the 2024-29 regulatory submission proposes to achieve these imperatives and enable TasNetworks' strategic business objectives by:

- *'Protecting the organisation's systems and services from cyber compromise, damage and unauthorised use;*
- *Protecting the organisation's information assets from exploitation, to ensure confidentiality, integrity, and availability;*
- *Maintain the risk position of the organisation despite the increase in sophistication of attacks and an order of magnitude increase in attack surface; and*
- *Continue to address cyber security concerns by executing prudent and efficient change and controlling risk aligned with an AESCSF SP-3 maturity profile or equivalent.'*

3.2.3 TasNetwork's cyber security current state

79. In the current RCP, TasNetworks' cyber security focus has been on establishing governance and undertaking discovery to better understand the risks faced by TasNetworks. This includes by building a cyber security team[24] and [redacted] in accordance with the AESCSF.

3.2.4 Options considered by TasNetworks for managing cyber security obligations and risks

80. TasNetworks summarises its objective for the next RCP as '*maturing its cyber security capability, with a view to maximising value from existing assets and any future procurement and through process maturation and evolution…*allowing it to move [redacted]

81. TasNetworks considered three options, selecting Option 1 ($8.1m capex and $21.6m opex , including an opex step change of $19.3m) across the Transmission and Distribution networks:

- Option 0: Do nothing ($2.6m);
- Option 1: Progressing in [redacted] ($29.7m); and
- Option 2: Uplift [redacted] ($73.0m).

[23] TasNetworks IES for Cyber Security Program of Work (R24), p10

[24] New roles include security architecture, risk analyst, security analysts and operational technology specialist,

4 OUR ASSESSMENT

We consider that TasNetworks' cyber security program objectives are reasonable and its targets are adequately justified.

We consider that TasNetworks' cost forecast is reasonably derived, however it includes some expenditure items that are not cyber security related. We propose an adjusted allowance for both capex and opex step change, which would also remove elements of a proposed contingency and which make a corrected adjustment to $2023/24 terms.

4.1 TasNetworks' risk analysis

82. TasNetworks has provided a qualitative risk analysis in its IES. In this section we assess whether the risk analysis is sufficiently compelling to support the proposed cyber security investment in the next RCP. TasNetworks' risk analysis also provides a framework for determining the appropriateness of its selected option in mitigating the risks, which we consider in section 4.3.

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

83. TasNetworks' Investment Evaluation Summary ('IES') includes a reasonably comprehensive and relevant risk analysis, considering five dimensions of cyber security risk:

- International cyber security threat landscape, with evidence of the rise of cyber-attacks in the global electricity sector;
- National cyber security threat landscape, with evidence of cyber security attacks on businesses;
- Increased attack surface of TasNetworks' electricity assets (network, OT and IT), due to the interconnectedness of the national grid and of TasNetworks' transmission network as part of this grid;
- Increased attack surface of TasNetworks assets due to the integration of an increasing number and type of distributed energy resources; and
- Increased attack surface due to other connections with third and fourth parties (e.g. suppliers).

84. We consider that TasNetworks' qualitative risk assessment reasonably concludes that the existing [redacted] and that it is likely to [redacted] without action by the end of the next RCP, if not before. Absent investment to increase TasNetworks' level of cyber preparedness, TasNetworks presents a reasonable case that there would be an increasing risk of a successful cyber security breach, leading to one or more of the identified events occurring (e.g. theft of personal or commercially sensitive information, interruption to supply), and increasing consequences should such a breach occur.

TasNetworks identifies high level cyber security-related compliance obligations but does not identify them in any detail

85. Whilst not included in its list of eight risks denoted in Section 3.2, a related Energy Policy and Regulation risk is separately identified as follows:[25]

[25] TasNetworks IES for Cyber Security Program of Work (R24), page 17

'Non-compliance with the Security Legislation Amendment and Privacy Act will impact business revenue and reputation through financial penalties plus business information being disclosed publicly in court proceedings.'

86. The proposed project is said by TasNetworks to indirectly support the mitigation of this risk, and which we consider to be a likely outcome, but nevertheless a vague statement. As discussed in Section 2, there are a number of dimensions to the SOCI Act and Privacy Act amendments which create obligations on TasNetworks (and other NSPs) and we observe that not all of these are clearly identified by TasNetworks in its IES.

TasNetworks concludes that its inherent cyber security risk rating is [redacted] which is reasonable

87. As a transmission and distribution network business, TasNetworks has assessed its risk rating to increase from [redacted]. We consider this to be a reasonable conclusion and which justifies the need to undertake further investment over the next RCP in order to maintain its current risk level.

4.2 TasNetworks' cyber security-related objectives

TasNetworks has designed its project not only to comply with its minimum regulatory obligations but to also reduce cost.

88. TasNetworks makes several statements regarding its objective to proactively manage its cyber security risks, protecting its critical assets in the process, *and* managing its compliance obligations.

89. As shown in Figure 4.1, its work in the current RCP has been (and still is) focused on compliance, risk identification, and defence. Its objectives for the next RCP are not explicitly couched in terms of merely meeting its compliance obligations.[27]

90. The IES also includes several statements which indicate an objective of its proposed investment is cost reduction:

"This is a primary objective of the project, to provide a secure technology platform the business can leverage to capitalise on innovation and reduce cost."[28]

'It is recommended this journey continues into R24 to uplift the cyber security capability and maturity as well as introduce efficiency improvements.'[29]

91. This indicates that TasNetworks is investing to reduce cost, not just to maintain its risk level (and meet its compliance obligations) and that there will be an efficiency dividend from the project. It is not clear whether these additional objectives have significantly influenced the design and cost of the project. This has implications for our assessment of the proposed expenditure against the NER criteria.

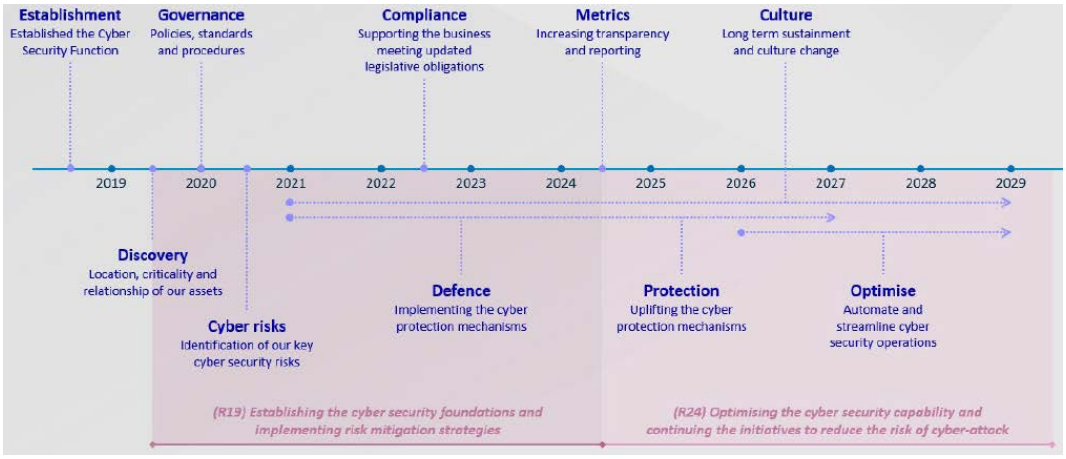
26 [redacted]

27 TasNetworks IES for Cyber Security Program of Work (R24), Figure 4

28 TasNetworks IES for Cyber Security Program of Work (R24), page 18

29 TasNetworks IES for Cyber Security Program of Work (R24), page 10

Figure 4.1: TasNetworks' cyber security journey



Source: TasNetworks IES for Cyber Security Program of Work (R24), Figure 4

TasNetworks is aiming to [redacted] by the end of the next RCP

92. TasNetworks' target cyber security maturity by the end of the current RCP is to have achieved [redacted]

93. One of its objectives (or 'cyber imperatives') is '*…maturing the Cyber Security function within TasNetworks* [redacted]

94. As discussed further in section 4.3, this is also couched in the context of '*maintaining its risk profile (and improving wherever possible)*'.

95. Given that TasNetworks is both a TNSP and a DNSP, we consider that investment to achieve a maturity level [redacted] is reasonable in the face of rising risks, provided there is adequate supporting justification (which we consider in Section 4.3).

4.3 TasNetworks' options analysis

96. TasNetworks considered three options as recorded in its IES. We discuss the merits of each below.

4.3.1 Option 0 – 'Do nothing'[31]

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

97. The cost of Option 0 over the next RCP is estimated to be $2.6m opex due to an uplift in the Cyber Security Team's overhead expenses (because the seven exiting team members would not be able to charge some of their time to the proposed Cyber Security Program).

98. Option 0 is positioned as the counterfactual for Options 1 and 2 and as such the avoided cost of a cyber security breach(es) during the next RCP is credited to those options as a benefit compared to Option 0, rather than including it as a dis-benefit for Option 0.

TasNetworks reasonably concludes that this option is not prudent

99. TasNetworks' qualitative risk analysis reasonably concludes that Option 0 will lead to a [redacted] by the end of the next RCP due to increasing attack sophistication and TasNetworks' increasing attack surface, as summarised in section 4.1. Given

30 TasNetworks IES for Cyber Security Program of Work (R24), page 19

31 While referred to colloquially as a 'do nothing' option, this option is more accurately described as 'continuing current policies and practices'

32 [redacted]

TasNetworks' risk appetite and compliance obligations as a Transmission and Distribution NSP, we consider it reasonable to assume that this increase in cyber security risk would not be not tolerable.

4.3.2 Option 1 (recommended by TasNetworks)

Project objectives are consistent with the needs that TasNetworks has identified in its risk assessment

100. In summary, the objectives of the option that TasNetworks proposes are:[33]

1. *Sustaining delivery of Transmission and Distribution services at or above the tolerances of the regulator;*
2. *Enabling the organisation to successfully execute its strategic vision securely;*
3. *Maintaining the risk of cyber incidents that could result in operational impacts to TasNetworks*
4. *Building capability to increase cyber maturity in line with recommendations for critical infrastructure service providers;*
5. *Embedding cyber security practices across the organisation (imbedding security by design) to prevent disruptions to business operations and/or loss of data; and*
6. *Transitioning cyber security awareness, training and testing to long term sustainment and culture change.*

101. These objectives are consistent with the needs that TasNetworks' risk assessment identifies. Further, we consider that TasNetworks' risk assessment is consistent with government agency and other sources of industry risk analysis.

[redacted] is open to interpretation but aligns with the AESCSF criticality positioning

102. As TasNetworks is aiming to [redacted] by the end of the current RCP, it will have what can be regarded as a 'managed' level of cyber security maturity (compared to what could be regarded as an 'ad hoc' approach to cyber security at [redacted]).

103. In response to the rising cyber security risk level that would not be addressed with Option 0, Option 1 is [redacted] by investing in prioritised cyber security practices that [redacted] coverage (either largely or fully implemented).[34] This is consistent with the 'prioritised practices' approach promulgated by the ACSC, as discussed in section 2.3.

104. Based on the AESCSF criticality bands (Figure 2.2), as a Transmission and Distribution business, TasNetworks could arguably [redacted] Based on the descriptions in its IES and supporting documentation Option 1 is targeting [redacted] practices (per AESCSF V1) by 2029 . The cost difference between largely implemented practices and fully implemented is significant, as discussed in our assessment of Option 2.

The Option 1 initiatives are clearly identified and mapped to the risks and AESCSF domains

105. TasNetworks identifies 15 initiatives in its IES. The initiatives are mapped by TasNetworks against the 11 AESCSF domains.

106. Based on TasNetworks' descriptions of the initiatives (including the mapping to the risks and AESCSF domains) and its asset criticality we consider that they are appropriate for TasNetworks as a Transmission and Distribution business. Notably,

---

33 TasNetworks IES for Cyber Security Program of Work (R24), page 19

34 [redacted]

- Three of the initiatives will be implemented by the commencement of the next RCP but will require ongoing maintenance and upgrades; and
- The initiatives include two scope areas in addition to AESCSF [redacted] capabilities to:
  - address the identified list of TasNetworks' risks, and increasing maturity against the ACSC Essential Eight
  - provide for 'Legislative governance requirements (SoNS)'. TasNetworks states that *'…if TasNetworks is declared a SoNS, this initiative is to address the following obligations: annual reporting, incident response planning, scenario-based exercising, vulnerability assessments, provision for access to information systems, etc.'*

107. The AESCSF V1 incorporates Essential Eight requirements but TasNetworks is aiming for Essential Eight [redacted] for all mitigation strategies, following the lead from the draft Rules. Similarly, making provision for the implications of being designated a SoNS (i.e. a potential obligation rather than a 'certain' obligation) does not strictly satisfy the AER guidelines. [redacted]

108. As shown in Table 3.1, the proposed expenditure on these two additional scope areas is relatively modest at a combined $360k over 5 years. We consider them to be reasonable provisions.

4.3.3 Option 2

109. Option 2 addresses the transformation projects and FTE uplift and includes all the activities from Option 1, as well as enhancements for establishing and maintaining automated operating effectiveness for key [redacted] controls and practices. The estimated incremental totex compared to Option 1 is $43.3m ($FY22).

> *'The initiatives in scope for option 2 centre around uplift in the OT environment, better control of the application environment, and increasing automation that can be leveraged to increase reliance cadence for operating systems, software and patches throughout both IT and OT.'*[36]

TasNetworks reasonably concludes that this option is not prudent

110. TasNetworks deems the cost is too great despite the merit and value in the initiatives and reducing the overall risk position. Option 2 is not TasNetworks' preferred option and we concur with its conclusion.

111. The remaining sections of this report refer by default to TasNetworks' preferred option (that is, option 1).

4.4 TasNetworks' cost forecasting methodology

Contingency adjustments are not fully justified

112. With the exception of inclusion of a 20% contingency estimate for its capex forecast and 30% for its opex forecast, we consider TasNetworks' cost forecasting methodology is reasonable.

113. For the capex contingency, TasNetworks' rationale is that increased costs may arise from:

- Changing obligations;
- The rate of change of new technology;

35 [redacted]

36 TasNetworks IES for Cyber Security Program of Work (R24), page 19

- Scarcity/competition for skilled resources; and
- The elevated and increasing cyber risk.

114. We consider that the capex contingency amount is not warranted, because:

- By targeting a risk mitigation level that is considerably above its minimum compliance level, we consider that TasNetworks will have some headroom in the event that bar is raised for those minimum regulatory compliance obligations,
- The costs of significant additional regulatory obligations can be sought via a pass through if they cannot be absorbed within TasNetworks' Level 1 estimate,
- We consider that the cost of new technology is more likely to reduce, not increase costs, and
- There is nothing in TasNetworks' cost estimation approach to suggest that it has not allowed for the 'scarcity' based cost of skilled resources.

115. TasNetworks' rationale for adding a 30% opex contingency amount is also based on the likelihood of higher FTE costs (to attract and retain) than the base levels assumed, and additional regulatory obligations. Based on PwC's benchmarking advice to TasNetworks, we consider that it is likely TasNetworks will experience additional cost; but we consider that a 30% loading is excessive and TasNetworks has not provided adequate justification for this amount.

Non-cyber security expenses should not be included in the cost estimate

116. TasNetworks has included $0.8m opex for addressing Personnel Hazards and $0.45m opex for addressing Physical Hazards. These are not cyber security-related and we propose that the cost is removed from TasNetworks opex forecast.

Other aspects of TasNetworks forecasting methodology are reasonable

117. Otherwise:

- The 'Level 1' estimate accuracy of ±20% is appropriate at this stage of the project lifecycle;
- TasNetworks has provided quite granular information (i.e. at the initiative level and across time);
- It has provided an explicit set of assumptions which, with the exception of the contingency provisions, are reasonable;
- It has incorporated external advice to both challenge its content (initiatives) and cost estimates using a combination of bottom-up costing and benchmarking; and
- The ratio between capex and opex (1:3) is reasonable, having been explained as follows:
  - A shift to ongoing maintenance (including licencing and support) and enhancement of process and technology, beyond the initial implementation phase;
  - increased subscription models for cyber tools and instrumentation;
  - increased staff to manage ongoing BAU requirements in comparison to non-recurrent delivery effort (capex and opex).

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

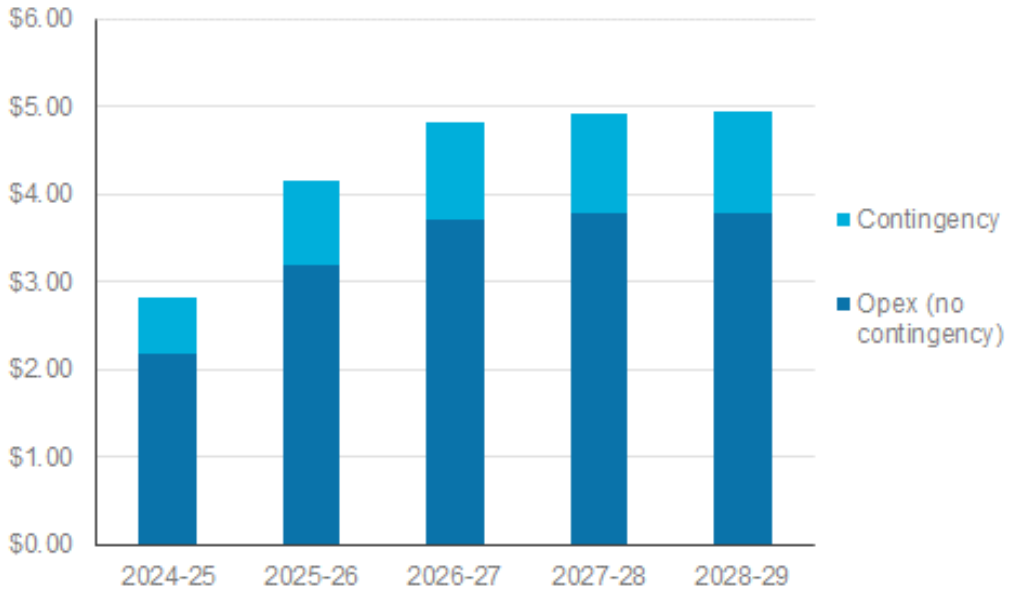
118. A potential source of cost increase is the updated (V2) of the AESCSF. For example, additional practices are likely to be included in V2.

119. To the extent that any such requirements become evident and are not already accounted for, we assume TasNetworks will take AESCSF V2 into account in its revised RP or through a pass-through.

Derivation of the Option 1 opex step-change of $19.3m is appropriate

120. TasNetworks has provided a 'bottom-up build' of its opex forecast of $21.6m ($FY22, including contingency of 30%) over the next RCP, distinguishing between labour effort, resource/FTE uplift, and support/maintenance/ subscription costs, leading to the opex profile shown in the diagram below.

Figure 4.2: TasNetworks' proposed opex forecast over the next RCP ($m, real 2022)



Source: TasNetworks-IR016-ICT Non-network Cyber (CYBRC) – Cost Estimate-20230414-Condidential

121. We consider that the subscription costs forecast to be incurred over the next RCP is likely to be recurrent and materially represent a capex to opex trade-off in moving to off-premise/cloud based services.

122. In response to an information request, TasNetworks also provided a spreadsheet showing the reconciliation of its $21.6m opex forecast over the next RCP (in $FY22) to its opex-step change amount of $19.3m over the next RCP, deducting the base year FY22) cyber opex of $1.086m ($FY22) from its forecast.[37] This reconciliation provides reasonable confirmation of its proposed opex step change.

Aside from inclusion of two non-cyber security roles the proposed additional FTEs will lead to a reasonable in-house cyber security capability

TasNetworks currently has [redacted] cyber security positions[38] and it has proposed an additiona[redacted] with an expenditure profile shown in the figure below.[40] TasNetworks has included $6.5m ($FY22, no contingency) over the next RCP for the increased FTE cost over and above the current FTE costs that exists within the Base Year.[41]

123. For estimating purposes, the expenditure profile indicates that the full complement of FTEs will be on-board from FY27 onwards. The roles are spread over what appears to be a

37 TasNetworks-IR039-Cyber step change reconciliation-20230623-Confidential

38 TasNetworks-PWC-Cyber Security Expenditure Review-Nov-22-Confidential, page 48

39 TasNetworks-Cyber Security Program of Work Investment Evaluation Summary-Oct 22-confidential, Table 8

40 This profile differs significantly from the profile that would apply with the commencement dates nominated in Table 8 of the IES, however TasNetworks advised in a response to an Information Request that the timing of the roles included in its CBA model was more likely due to delays in resource acquisition

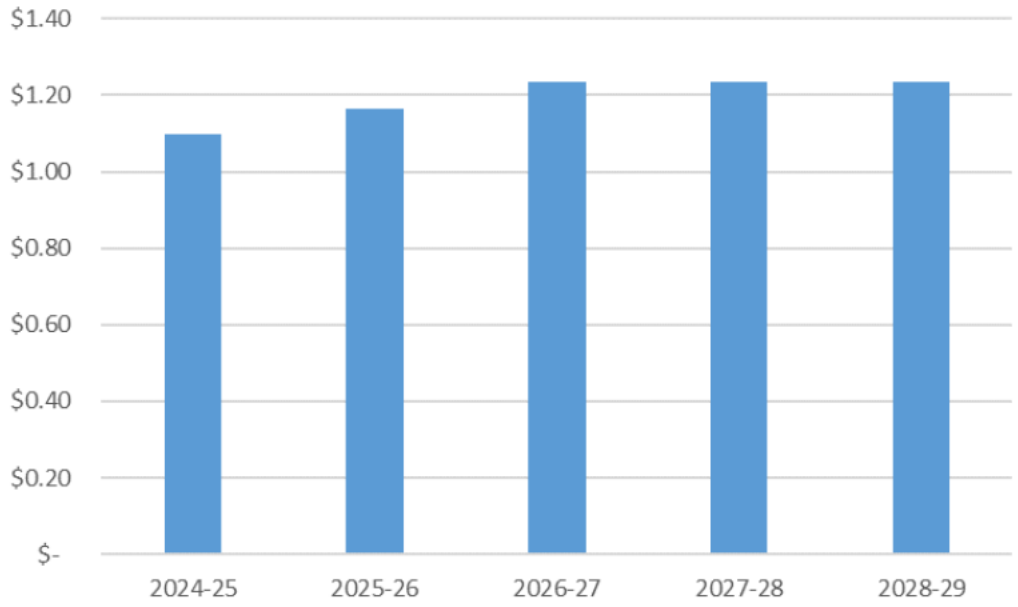
41 TasNetworks response IR042 – Opex – Cyber security step change, question 2 and TasNetworks-IR016-ICT Non-network Cyber (CYBRC) – Cost estimate-20230414-Confidential, Expenditure profile worksheet

dedicated cyber security team, IT, HR (people and culture), and Procurement/Fleet/Facilities functions.

124. In relationship to the proposed new roles in Table 8 of its IES, we consider that:

- Out-posting roles in various departments/functions is a reasonable approach;
- TasNetworks inclusion of 0.5FTE for a Physical Security Officer (in the Procurement/Fleet/Facilities function) and 0.5 FTE for a Personnel Vetting Officer are not appropriate for the cyber security opex step change because they respond to other aspects of the SOCI Act amendments;[42] and
- To [redacted] a cyber security team of [redacted] is reasonable (supported by external specialists for specific tasks from time to time), nominally comprising [redacted] plus the Chief Cyber Security Officer (aka the head of the cyber security team).[43]

Figure 4.3: Additional opex from additional FTEs ($m, real 2022)[44]



Source: TasNetworks-IR016-ICT Non-network Cyber (CYBRC) – Cost Estimate-20230414-Confidential

125. On balance, we consider that TasNetworks' proposed FTE contribution to the opex step change is overstated by one FTEs or $0.7m over 5 years (using the average of $138.5k per role p.a. average cost).

Inclusion of $1.0m for an incident response retainer is reasonable

126. TasNetworks has included $0.2m pa ($FY22 and without contingency loading) over the next RCP as a retainer for an incident response expert. We consider this a reasonable provision on the basis that the retainer reduces the consequence cost if a cyber security breach occurs.

42 This is not a conclusion that the additional FTEs (or part thereof) are not required

43 The role of the cyber security team is typically not to operate the IT systems, but to enforce cyber policies and standards, manage and operate the cyber risk register, run assurance and test the technical controls, and remediate gaps in the protection/resilience components of technology; the cyber controls such as perimeter security, identity services, patching programs are operated by IT

44 Figures are inclusive of on-costs and exclusive of contingency

4.5 Other aspects

4.5.1 Economic justification

TasNetworks' benefit forecast is insufficient to deliver a positive NPV but Option 1 is still the logical choice for TasNetworks (albeit at a reduced cost)

127. As discussed elsewhere, because we consider that the totex proposed by TasNetworks is primarily directed towards maintaining the risk level, not improvement, it is not strictly necessary for TasNetworks to demonstrate a positive NPV for its project.

128. TasNetworks has provided a cost-benefit analysis which, among other things, includes an avoided cyber breach ('risk abatement') cost of [redacted] over the 10 year CBA study period) as a benefit for Options 1 and 2. TasNetworks does not provide a detailed explanation of the basis for the estimate.[45]

129. Based on our experience, if a significant cyber-attack is successful:

- The cost to sanitise and re-build the affected systems, including the forensic analysis, and resetting would be in the range $3m-$9m for a business of TasNetworks' size and complexity;
- Cost to remediate security gaps would be in the order of $1m - $5m;
- Whilst there may be a ransom request, we have not factored this in on top of the above range estimates;
- Whilst there may be loss of revenue, we have not factored this in on top of the above range of estimates;
- It is not reasonable to assume that there will be a successful breach every year – [redacted]

130. We consider that it would be reasonable to assume:

- A risk abatement benefit in the range $4m-$14m over 5 years or $8-$28m over a 10 year CBA study period; and that
- For the purposes of CBA modelling, a midpoint estimate of $18m over 10 years or $1.8m p.a. would be reasonable.

131. We therefore consider that TasNetworks' estimate is at the high end of a reasonable range, but it is not unreasonable.

132. Applying a lower annual benefit of $1.8m pa would increase the net present costs (NPC) of Options 1 and 2, however the relativities between the two would remain. The NPC of Option 0 will remain significantly less than Option 1, but we would still not consider it to be the prudent approach.

4.5.2 Timing

Timing of the initiatives is reasonable but there appears to be considerable implementation risk

133. TasNetworks has provided a completion timeframe for 11 of the proposed initiatives and a detailed description of the implementation (delivery) risks, but not the mitigating controls. In aggregate, there are significant risks to completing the project within the next RCP. Although a risk rating is not offered by TasNetworks, from the description [redacted]

[45] It does reference 'How to measure Anything in Cybersecurity Risk (D. W. Hubbard and R. Seiersen) and Factor Analysis of Information Risk (FAIR) modelling (international standard quantification model for information security and operational risk) but without further detail

134. Without a satisfactory description of the delivery risk controls, we infer that TasNetworks is placing significant reliance on (i) building its internal capability, and (ii) a hybrid resourcing model for the development and implementation phases of the initiatives. We note however that attraction and retention of specialist staff is a 'an increasing challenge.'

135. We therefore consider that [redacted]

4.5.3 Cost allocation between transmission and distribution

Cost allocation between Transmission and Distribution is appropriate

136. TasNetworks states that: *The cost allocation split utilised is 80% to transmission and 20% to distribution as this reflects the underlying consequence rating for our aggregated cyber risks which is appropriate for the majority of the initiatives.'*[46]

4.6 Our findings and implications

4.6.1 Summary of our findings

TasNetworks' proposed cyber security program is designed to allow it to maintain its current risk level. This is an appropriate objective, and its prioritised approach and targets are adequately justified.

137. TasNetworks provides a satisfactory case for responding to increasing cyber security risk over the next RCP.

138. TasNetworks has compliance obligations arising from amendments to the SOCI Act and the Privacy Act, however, it has not designed its project to only comply with its regulatory obligations. Rather its cyber security investment strategy is predicated on [redacted] during the next RCP.

139. In accordance with the AER ICT capex assessment guidelines, we have therefore considered the prudency and efficiency of TasNetworks' proposed cyber security forecast to address broader risk than its compliance obligations.

140. TasNetworks is aiming to [redacted] by the end of the next RCP, which we consider appropriate for TasNetworks given that the proposal covers transmission and distribution network services.

Inclusion of the capex contingency is not justified, the provision for increased resource costs is excessive, and non-cyber expenses should not be included.

141. TasNetworks' cost forecasting methodology is appropriate except for the inclusion of contingency adjustments and non-cyber expenses:

- The reasons for including the capex contingency of 20% are not compelling; and
- We consider that it is reasonable to include a real cost escalation of an average of 20% over the next RCP to account for TasNetworks likely incurred costs in recruiting and retaining scarce cyber security FTEs in lieu of the proposed 30% contingency and the removal of two 0.5 FTE non-cyber security roles from the cyber security opex step change estimate.

The opex step change may be considered not to strictly meet the requirements of AER's guidelines, but we consider that it is prudent

142. We also recognise that TasNetworks' proposed opex step change is based on more than responding to (i) its new compliance obligations and/or risks arising from amendments to the

[46] TasNetworks' response to Information Request IR009

SOCI Act and the Privacy Act, and (ii) trade-offs from moving from capex (on-premise tools and systems) to off-premise/hosted services incurring opex. It proposes an incremental opex uplift to maintain its cyber security risk level. This may be considered not to strictly meet the requirements of AER's guidelines, but we consider that it is prudent.

4.6.2 Implications of our findings for proposed expenditure

143. Table 4.1 and Table 4.2 summarise our proposed adjustments. As shown, the adjusted capex and adjusted opex step changes are applied to TasNetworks' transmission and distribution businesses in the proportion 80:20, as TasNetworks proposed.

Table 4.1: EMCa proposed adjustment to TasNetworks proposed cyber security capex ($m)

Description	2024/25	2025/26	2026/27	2027/28	2028/29	Total
TasNetworks proposed capex ($2021/22)	1.60	1.90	2.00	1.60	0.90	**8.10**
TasNetworks proposed capex ($2023/24)	1.76	2.09	2.20	1.76	0.99	**8.90**
Deduction of contingency of 20%	*-0.35*	*-0.42*	*-0.44*	*-0.35*	*-0.20*	***-1.78***
Adjusted cyber security capex ($2023/24)	**1.41**	**1.67**	**1.76**	**1.41**	**0.79**	**7.12**
Transmission allocation	*1.12*	*1.34*	*1.41*	*1.12*	*0.63*	***5.69***
Distribution allocation	*0.28*	*0.33*	*0.35*	*0.28*	*0.16*	***1.42***

Source: EMCa analysis from information provided as shown in Table 3.1, and with reference to TasNetworks IR#039 reconciliation response

Table 4.2: EMCa proposed adjustment to TasNetworks proposed cyber security opex step change ($m)

Description	2024/25	2025/26	2026/27	2027/28	2028/29	Total
TasNetworks proposed cyber opex ($2021/22)	2.83	4.15	4.81	4.91	4.93	**21.63**[47]
EMCa reduction for non-cyber components	*-0.33*	*-0.33*	*-0.33*	*-0.33*	*-0.33*	***-1.63***
Opex adjusted to remove non-cyber components	2.50	3.83	4.48	4.58	4.61	20.00
Further deduction of 10% 'excess' contingency	*-0.23*	*-0.35*	*-0.41*	*-0.42*	*-0.42*	***-1.82***
Opex adjusted after deduction of 10%	2.28	3.48	4.08	4.17	4.19	18.19
less base year ($2021/22)	*-1.09*	*-1.09*	*-1.09*	*-1.09*	*-1.09*	***-5.43***
Adjusted opex step change ($2021/22)	1.19	2.40	2.99	3.08	3.10	12.76
Adjusted opex step change ($2023/24)	**1.31**	**2.63**	**3.28**	**3.38**	**3.41**	**14.01**
Transmission allocation	*1.05*	*2.10*	*2.62*	*2.70*	*2.73*	***11.21***
Distribution allocation	*0.26*	*0.53*	*0.66*	*0.68*	*0.68*	***2.80***

Source: EMCa analysis from information provided as shown in Table 3.2, and with reference to TasNetworks IR#039 reconciliation response

[47] As we note in section 3.1, this is the amount that TasNetworks advised in its response to IR#039 reconciliation, along with the base year opex of $5.43m deducted below (both in $2021-22 terms).