EMCa

energy market consulting associates

Regulatory Submission for period 2021/22 to 2025/26

AUSNET SERVICES - REVIEW OF PROPOSED OPEX ICT-RELATED STEP CHANGES

Report prepared for:

AUSTRALIAN ENERGY REGULATOR

August 2020

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be applied to the prescribed distribution services of AusNet Services from 1st July 2021 to 30th June 2026. 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.

This report relies on information provided to EMCa by AusNet Services. 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 EMCa prior to 31st July 2020 and any information provided after this time may not have been taken into account.

Enquiries about this report should be directed to:

Paul Sell
Managing Director
contact@emca.com.au

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

Date saved
24/09/2020 9:53 AM

Version
Final v4

Energy Market Consulting associates
ABN 75 102 418 020

Sydney Office
802/75 Miller Street, North Sydney NSW 2060
PO Box 592, North Sydney NSW 2059
+(61) 2 9929 6274
contact@emca.com.au
www.emca.com.au

Perth Office
Level 1, Suite 2 572 Hay Street, Perth WA 6000
+(61) 8 9421 1704
contact@emca.com.au
www.emca.com.au

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS

Term	Definition
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
ASIC	Australian Security & Investment Commission
BAU	Business as Usual
CIS	Customer Information Services
CRM	Customer Relationship Management
DNSP	Distribution Network Service Provider
ICT	Information and Communications Technology
MIL	Maturity Indicator Levels
NER	National Electricity Rules
NPV	Net Present Value
OMS	Outage Management System
RCP	Regulatory Control Period
RIN	Regulatory Information Notice
SP	Security Profile
TNSP	Transmission Network Service Provider

1 INTRODUCTION

1.1 Scope

1. The AER has asked for EMCa's advice on two ICT-related opex step changes that AusNet Services (AusNet) has proposed as part of its Regulatory Proposal for the period 2021/22 to 2025/26. These are for:

- Proposed additional cyber-security related opex; and
- Proposed additional opex for migration of its core infrastructure systems and applications to the cloud.

1.2 Our approach

2. Our approach involved:

- Reviewing those aspects of AusNet's Regulatory Proposal and associated supporting documents in which it proposes the additional opex costs and step change;
- Meeting with AusNet by video-conference, in conjunction with AER staff, on 3rd June 2020; and
- Reviewing follow-up information provided by AusNet in response to Information Requests.

1.3 Presentation of expenditure amounts

3. Expenditure is presented in this report in $2021 real terms, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.

4. AusNet has proposed expenditure allowances which it has real-cost escalated in aggregate. However, project and program-level information presented by AusNet (such as in its project models and business cases) has generally not had escalation applied. Accordingly, in this report, we have presented expenditure information in non-escalated terms to preserve comparability with the source data. We have footnoted any graphs and tables that comprise non-escalated expenditure.

5. Whilst we have endeavoured to reconcile expenditure amounts presented in this report to source information, in some cases there may be discrepancies in the source information and minor differences due to rounding. Any such discrepancies do not affect our findings.

2 AUSNET'S PROPOSED CYBER SECURITY OPEX STEP CHANGE

AusNet plans to achieve a cyber-security level [redacted] which is appropriate for an electricity distribution business. AusNet expects to reach this level by [redacted]

AusNet subsequently plans to achieve [redacted] AusNet proposes to allocate this additional cost between its electricity transmission, electricity distribution and gas pipeline businesses. Since the Distribution business comprises 17% of total AusNet customers, AusNet proposes a 17% allocation of the incremental cost of achieving [redacted] AusNet proposes to recover the allocated distribution costs of $4.5m through an opex step change.

We consider that AusNet has not made the case [redacted] We therefore consider that the proposed opex step change is not warranted.

2.1 Introduction

7. AusNet proposes to continue to invest in systems to identify, protect, detect, respond, and recover from cyber-attacks. AusNet has submitted information to support recurrent and non-recurrent investments in new cyber security-related capabilities across its regulated Transmission, Distribution and Gas utility businesses.

2.2 AusNet's proposed cyber security program

2.2.1 Overview of proposed program

AusNet's cyber security program covers all three of its utility service providers

8. AusNet's utility services business is comprised of a transmission electricity network service provider (Transmission), a distribution electricity network service provider (Distribution) and a gas distribution service provider (Gas). The assessment in this section involves the allocation of proposed cyber security expenditure in the next RCP to all three utility businesses; however, our conclusions relate only to the expenditure allocation that is proposed for the Distribution business.

AusNet has structured its proposed expenditure on achieving benchmarks set in the AESCF

9. In reviewing AusNet's cyber security program and, in particular, its proposed opex step change, reference is made to the Australian Energy Sector Cyber Security Framework (AESCSF). This framework has been applied by AusNet as a basis for cyber security maturity assessment (or resilience to cyber threats).

10. The development of the AESCSF was led by the Australian Energy Market Operator (AEMO) in conjunction with industry and government stakeholders.[1] It provides a self-assessment framework for measuring cyber security maturity according to three gradings of Maturity Indicator Levels (MIL): MIL 1; MIL 2; and MIL 3, with the latter being the highest level. The AESCSF comprises 11 domains, 28 objectives 240 practices and 42 anti-patterns.

11. It is common for electricity utilities to self-assess their progress (with or without external advice), including partial progress, towards achieving any of the three MILs. [redacted]

12. In the latest version of the AESCSF framework (version 2019-8), Security Profile (SP) levels 1-3 have been introduced. Our understanding is that 'MIL2/SP-2' and 'MIL3/SP-3' levels represent the equivalent cyber security maturity.

13. In this report, we refer only to MILs because this is the basis for AusNet's proposed cybersecurity capex and opex program for the next RCP (i.e., AusNet's proposal was developed prior to the latest version of the AESCSF that included SP levels).

2.2.2 AusNet's proposed capex and opex

14. AusNet has proposed [redacted]

[redacted]

2.2.3 AusNet's justification for its cyber security opex step change

Cybersecurity threats are increasing

16. AusNet observes that there is an increase in cyber-threats to the electricity sector and that it has regulatory obligations to respond to these threats:[3]

> *'As a regulated entity, Australian Security & Investment Commission (ASIC) requires the disclosure of information in the event of a cyber-attack. The current and emerging regulatory cyber security laws and guidelines require ongoing organisational response and compliance. These include the Security of Critical Infrastructure Act 2018, Notifiable Data Breaches Act 2017, Privacy Act 1988, EU General Data Protection Regulation, and*

1 Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC), and the Cyber Security Industry Working Group (CSIWG); the latter includes representatives from Australian energy organisations

2 [redacted]

3 [redacted]

Security of Critical Infrastructure Bill 2018. As well as the ASIC Cyber Resilience: Health Check, Report 429, released in 2015; and

For AusNet Services, threats are multi-fold such as cyber terrorism, denial of service, extortion and cyber vandalism. With the introduction of Distributed Energy Resources and Advanced Metering Infrastructure, the number of connection points into the network has increased. Each of these connection points can act as an attack vector if the perpetrators manage to compromise devices such as meters, either by modifying the electricity consumption data or to get into the network.'

[redacted]

4 [redacted]

5 [redacted]

6 [redacted]

7 [redacted]

[redacted]

Options selection methodology

26. AusNet applied qualitative and quantitative assessment methodologies to select its preferred option.

27. Its qualitative assessment comprises a scoring system that is aligned to '*achieving AusNet's business and customer objectives as well as requirements of the AER in ensuring that any expenditure is both prudent and efficient.*'[13]

[redacted]

8 [redacted]

9 [redacted]

10 [redacted]

11 [redacted]

12 [redacted]

13 [redacted]

14 [redacted]

2.3 Our assessment

[redacted]

30. In addition to the information presented by AusNet in its Regulatory Proposal and in its Cyber Security Technology Program, our industry experience confirms that cyber threats are escalating. As recently as 19 June 2020, the Australian Prime Minister announced that there had been a cyber attack by a '*sophisticated state-based actor… targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers, and operators of other critical infrastructure.*'[15]

31. We consider that there is sufficient evidence to underpin continuing focus by AusNet (and other Australian electricity utilities) on improving its cyber security resilience in the face of evolving cyber threats.

[redacted]

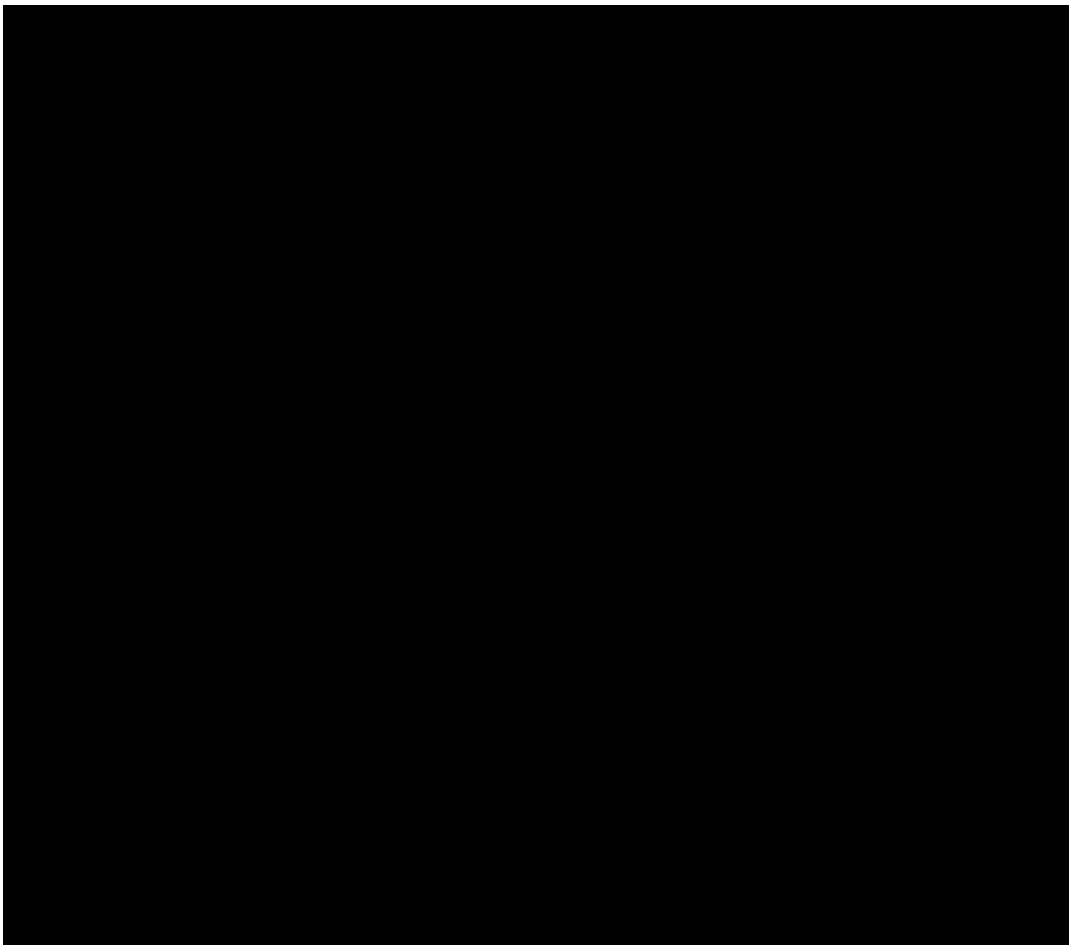
[redacted]

15 https://www.abc.net.au/news/2020-06-19/foreign-cyber-hack-targets-australian-government-and-business/12372470

16 AEMO Australian Energy Sector Cyber Security Framework (AESCSF) Framework and 2019 Self-Assessment Program Overview, Version 2019

17 AusNet Regulatory Proposal, pages 145-146

18 [redacted]



2.4 Implications for proposed cyber security opex step change

44. We are satisfied that:

- There is an escalating threat from cyber attacks such that it is prudent for AusNet to improve its cyber security posture;
- AEMO's guidance is that DNSP's are 'Moderately Critical' infrastructure organisations [redacted] and
- AusNet's strategy of [redacted]

45. [redacted]

19 [redacted]

20 [redacted]

21 [redacted]

22 [redacted]

23 [redacted]

- [redacted]
- [redacted]

3 IT CLOUD OPEX STEP CHANGE

In this section, we consider AusNet's proposed opex step change for cloud migration.

We consider that AusNet's proposed adoption of cloud-based solutions is likely to be the best approach for the selected applications to maintain currency and access to vendor support. However, AusNet states that there is not a capex trade-off in doing so and that the proposed opex step change is not driven by a changed external obligation. We therefore consider that AusNet's proposal does not satisfy the relevant NER criteria for an opex step change.

We consider that the opportunity remains for AusNet to undertake these migrations based on its internal commercial assessments.

3.1 Introduction

46. AusNet proposes an opex step change of $2.6m that it expects to incur as a result of its vendors changing to a cloud-hosted model from its existing capex-based on-premises applications model. In this section, we describe AusNet's rationale for the opex step change and assess the proposed opex in the context of the requirements of the NER.

3.2 AusNet's proposed IT cloud migration program

AusNet proposes to transition six systems and applications to cloud-based hosting in the next RCP

47. AusNet advises that it '*has undertaken a high level analysis of transitioning its core systems infrastructure to cloud'* and concludes that the '*…benefits of moving all services into the cloud during [the next RCP] are not large enough to outweigh the risks and costs of doing so…'* [24]

48. However, vendors for six applications have advised AusNet that all future versions of their applications will be cloud based. To '*maintain the currency and vendor support … AusNet Services needs to prepare for transition to the cloud'* of the applications listed in the table below at an estimated cost of $1.5m per annum of additional opex.[25]

[24] ASD – Appendix 9C Technology Strategy -181119, page 54

[25] *Ibid*

Table 3.1: AusNet Services systems and applications to be transitioned to cloud hosting in the next RCP - $000, real 2021

Technology Capex Program	Cloud hosting opex increase	Opex ($000 p.a.)
Outage management	Cognitive automation subscription	458
Customer Information Services	Customer Relationship Management System	50
Corporate Enablement	Human Resources and payroll management	225
Workforce Collaboration	Enterprise Knowledge Management Tool Project Portfolio Management	560
Information Management	Information Management Platform	209
TOTAL		**1,502**

Source: ANS Technology Strategy, Figure 6.8, page 54 modified by EMCa[26]; ASD - ASD - IR 037 (Q2) - Cloud based IT step change - Response to CF – 20200619 (Page 1)

AusNet proposes to absorb the majority of the opex step change

49. AusNet considered seeking the full estimated opex step change amount in its Draft Plan for the next RCP. However, it advises that the Customer Forum only agreed to $2.6 million in additional costs for: (i) the Customer Relationship Management (CRM) component of its Customer Information Services (CIS); and (ii) the cognitive automation subscription for its Outage Management system (OMS) to cloud-hosted service.[27] Consequently, AusNet proposes a step change of $2.6m (being approximately $0.5m p.a.) over the next RCP and will absorb the remainder of the cost (being approximately $1.0m p.a.).

3.3 Our assessment

The proposed Outage Management System NPV is only marginally positive

50. AusNet considered four options to '*reduce the impact of planned outages on customers to a minimal level, by using advanced analytics and automation across the workflow to improve process efficiency for planned works'* [28] as shown below:

- Option 0 - Do nothing;
- Option 1 - Data quality improvement;
- Option 2 - Process automation; and
- Option 3 - Integrated solution (Intelligent Automation).

51. AusNet states that '*Do Nothing is not an acceptable option for addressing planned outages over the next regulatory period* because its *ability to ensure that the value of available data is maximized is currently limited by the capacity of AusNet Services' current technology systems that are used to monitor the LV network and communicate with customers*.'[29]

---

26 AusNet's table also includes a description of corporate communications '*required to support cloud hosting for other applications*', however as AusNet Services has not identified an accompanying opex step change we have removed this row from the table

27 AusNet Services Regulatory Proposal 2022-26, page 146

28 ASD - Program Brief - Outage Management - 191119 – CONFIDENTIAL, page 5

29 ASD - Program Brief - Outage Management - 191119 – CONFIDENTIAL, page 13

52. AusNet selected Option 2 at a capital cost of $8.8m capex and $2.8m opex, with an opex step change of $50k p.a. for a cloud service for Cognitive Automation. It does not currently subscribe to this service.[30] AusNet advises that *'[t]he only alternative would be to custom build the capability in-house which is not prudent as it is cost prohibitive and not in line with AusNet Services' architectural principles or industry standard practices.'*[31]

53. If AusNet's investment in the proposed Outage Management improvement project proceeds, a cloud-based solution for the automation component is likely to be the sensible path given the lack of fit-for-purpose alternatives and the relatively cheap annual subscription cost.

54. Option 2 includes activities to improve data quality, asset maintenance modelling, forecasting capability and ongoing input of field data. It plans to utilise that data for automated processing of the end-to-end workflow (with the exception of switching instructions).

55. In response to a request for information from the AER, AusNet provided its NPV analysis for Option 2 in which it identifies a $0.15m NPV (7-year study period) based on two benefit streams:[32]

- reduced customer outage time valued at approximately $0.4m p.a.; and
- improved employed productivity (i.e., less time required from field staff responding to outages) also valued at approximately $0.4m p.a.

56. The NPV of Options 1 and 3 are -$2.3m and -$0.4m, respectively, which are therefore inferior on an NPV basis to Option 2.

57. As the values in the provided spreadsheet are hardcoded, it is difficult to verify the reasonableness of the claimed costs and benefits. However, we note that with such a small positive NPV for AusNet's preferred option, the NPV will be increasingly negative for unfavourable variances to key inputs. AusNet also identifies unquantified benefits from Option 2 in the spreadsheet as follows:

- improvement to data quality, improved asset maintenance modelling and forecasting capability, enhanced ongoing input of field data; and
- increased oversight and monitoring of asset performance, improved asset utilisation and increased asset life.

58. On the evidence presented, there appears to be a business case for the proposed Outage Management System and for AusNet's selection of Option 2. However, we consider that the NPV for this prospective investment is marginal.

The proposed CRM solution is likely to be a prudent solution

59. AusNet proposes to improve its Customer Information Services (CIS) by improving *'the interactions between AusNet Services and our customers, to visualise their energy use behaviour, and consumption profile, and to remain compliant with increasingly sophisticated regulatory rule changes around the collection, storage and distribution of customer information:'*[33] It considered three options:

- Option 1 - Business as usual;
- Option 2 - Implementing a subscription-based CRM system; and
- Option 3 - Transitioning to a dedicated Customer Information Management (CIM) solution, which includes implementation of an enterprise-wide CRM system.

30 This is 100% of the total cost for AusNet Services as a whole

31 ASD – Appendix 9C Technology Strategy -181119, page 18

32 ASD – IR037(Q4) – OM - 20200619

33 ASD - Program Brief Customer Information Services - 140120 – CONFIDENTIAL, pages 4, 13-14

60. AusNet selected Option 2 at a capital cost of $6.1m capex and $1.6m opex, with 60% of the cost of the subscription-based CRM cost allocated to electricity distribution. AusNet estimates an ongoing cloud-subscription fee of $$270k p.a. to distribution.[34]

61. AusNet advises that '*[c]ustomer information market products for organisations similar to AusNet Services are cloud based…mature and proven in the industry to improve communication and customer service through information, insights and accessibility…*' and that other benefits include *'scalability and agility as capacity requirements are handled automatically to allow for seamless change in response to demand*.[35]

62. In our view, a cloud-based solution is likely to be superior to on-premises alternatives.

63. In response to a request for information from the AER, AusNet provided its NPV analysis in which it identifies a $10.4m NPV (7 year study period), based on four benefit streams:

- improved employee productivity;
- reduction of customer time spent;
- reduction of customer time spent and costs obtaining cheques; and
- cost to customer of processing cheques.

64. The sources of benefits in the provided spreadsheet appear to be reasonable. We note that the spreadsheet contains hard coded values. Whilst the benefits are sensitive to several critical assumptions,[36] there is no evidence of AusNet having undertaken a sensitivity analysis to these assumptions.

65. Based on the relatively fast payback period for the investment and the quantum of the NPV with AusNet's input parameter assumptions, we consider it likely that the proposed program NPV will be positive with reasonable negative input parameter variances.

AusNet did not provide business cases or NPV analyses for the other three programs

66. AusNet's Technology Strategy provides the following justification for the other three programs:[37]

- 'HR and payroll management: *'[i]t is more prudent and efficient to leverage the existing vendor product suite, by extending existing cloud based capabilities implemented at AusNet Services, than invest in individual components of an alternative solution;*
- Workforce collaboration – *[c]ollaboration products for organisations similar to AusNet Services are cloud based. It is more prudent and efficient to leverage the existing vendor product suite, by extending existing cloud based capabilities implemented at AusNet Services, than invest in individual components of an alternative solution; and*
- Information management – *[e]xtension of capacity to existing cloud based capabilities at AusNet Services to enable rapid access to timely, accurate data across all critical systems, assets, processes, and support more advanced analytics and reporting.'*

67. AusNet did not provide supporting NPV analyses for these programs. Based on the information provided, we consider it likely that its selection of cloud-based solutions is a reasonable approach. However, as stated in section 3.2, AusNet has not included allowances for these three projects in its proposed opex step change.

AusNet's step-change does not satisfy the AER criteria for an opex step change

68. AusNet states that *'[t]his program meets the AER definition of a forecast opex step change as it is a capex/opex trade-off and results in lower capex in the next regulatory period*

---

34 Based on the proportion of AusNet's distribution customers to total electricity customers; AusNet Services, Program Brief Customer Information Services - 140120 – CONFIDENTIAL, page 19

35 ASD – Appendix 9C Technology Strategy -181119, page 18

36 Such as the number of payments made by cheque, which ANS assumes will be constant at 2,500 pa for the next 7 years

37 ASD – Appendix 9C Technology Strategy – 181119 – CONFIDENTIAL, page 18-19, noting that this document also includes qualitative justification for a Corporate Communications program which is not referred to in other sources

(compared to a counterfactual where we procure these as a capex solution).[38] In information presented to the Customer Forum, this statement is explained by reference to capital costs of more than $15m for the Workforce Collaboration program, more than $40m for the Information Management program and more than $9m for the HR and Payroll Management program.[39]

69. However, AusNet separately advises that the '*increase in opex associated with cloud hosting will not be offset by capex reductions in the next regulatory period because we share the hardware on which these applications run with other services and so are not able to decommission it yet.'*[40]

70. We consider that the lack of an avoided capital cost implies that the proposed expenditure does not satisfy the capex-opex trade-off criterion for an opex step-change in accordance with the AER's Expenditure Forecast Assessment Guideline.

71. The second criterion under the NER for an opex step-change is that the increased opex is driven by an external (regulatory) obligation. AusNet has not claimed that its step change satisfies this criterion.

72. We therefore conclude that the proposed opex step change does not satisfy the NER criteria.

3.4 Implications for proposed IT cloud opex step change

73. In our view:

- the proposed cloud-based hosting component of the OMS solution is likely to be the best approach to achieving the required functionality – however, the overall proposed OMS project is only marginally NPV positive; and
- the cloud-based CRM solution is likely to be the best approach to introducing the proposed functionality and the project NPV is positive even with reasonable negative variances to input assumptions.

74. However, we consider that the opex step change of $2.6m (approximately $0.5m p.a.) that AusNet Distribution has proposed for these two projects does not satisfy the relevant NER criteria as it is not: (i) offset by a capex reduction; or (ii) driven by a changed external obligation.

38 AusNet Regulatory Proposal 2022-26, page 147

39 ASD – IR 037 (Q2) – Cloud IT step change – Response to CF – 2020619

40 ASD – Appendix 9C Technology Strategy – 181119 – CONFIDENTIAL, page 54