Cyber security

CP BUS 7.04 - Cyber security - Jan2020 - Public

Regulatory proposal 2021–2026

CitiPower

January 2020

Contents

1 Overview

Business	CitiPower and Powercor Australia
Title	Cyber security
Project ID	CP BUS 7.04 - Cyber security - Jan2020 - Public
Category	IT capital expenditure - recurrent and non-recurrent
Identified need	We need to invest in uplifting our cyber security capability to enable us to support the safe and dependable delivery of electricity and protection of customers' personal information; provide foundational cyber security services that are flexible; and avoid the high costs of unplanned recovery and remediation efforts required in the event of a major/significant cyber incident.
Recommended option	Option 2 – maintain currency of existing security capabilities and optimise their effectiveness through an increase in scope of coverage
Proposed start date	2021/22
Proposed commission date	2025/26
Supporting documents	1. CP MOD 7.05 - Cyber security cost - Jan2020 - Public 2. CP MOD 7.06 - Cyber security risk - Jan2020 - Public 3. CP ATT047 - PWC - Cyber strategy review - Nov19- Public 4. CP MOD 12.02 - Quoted services labour rate - Jan2020 - Public 5. CP ATT195 - US DHS - Russian cyber activity - Mar2018 - Public 6. CP ATT192 - ACSC - Routers targeted - Apr2018 - Public 7. CP ATT186 - AEMO - 2018 Cyber security preparedness - Dec2018 - Public 8. CP ATT188 - HomeAffairs - Cyber security strategy - Nov2019 - Public 9. CP ATT197 - WEF - The Global Risks - 2019 - Public 10. CP ATT190 - US DHS - ICS alert-cyber attack against Ukraine - Feb2016 - Public 11. CP ATT196 - WEF - Cyber Resilience in Electricity Ecosystem - Jan2019 - Public 12. CP ATT189 - OAIC - Securing personal information - jun2018 - Public 13. CP ATT187 - OAIC - Data breach preparation and response - Feb2018 - Public 14. CP ATT185 - ACSC - Essential eight explained - Apr2019 - Public 15. CP ATT193 - EMV - Critical infrastructure resilience - Jul2015 - Public 16. CP ATT194 - EMV - Victoria's critical infrastructure - May2019 - Public 17. CP ATT191 - Alan Finkel - Future Security of the NEM - Jun2017 - Public

We are part of Australia's critical infrastructure and are responsible for the safe and reliable delivery of electricity to over 1.2 million homes and businesses. The traditionally separate domains of corporate information technology (**IT**) and industrial operational technology (**OT**) are increasingly interconnected as the digitalisation of the grid introduces new complexities and interdependencies. We rely on technology to safely operate and control the electrical network and this reliance will continue to increase over time as technologies continue developing.

Our cyber security program protects our network and helps us to maintain the quality, reliability, and security of electricity supply. Cyber threats against critical infrastructure continue to increase and the World Economic Forum (**WEF**) Global Risks Report 2019 includes cyber-attacks in the top five global risks by likelihood over a 10-year horizon. Cyber-attacks against critical infrastructure have also become increasingly sophisticated, with real-world impacts such as the unscheduled power outage in Ukraine in December 2015, which impacted approximately 225,000 customers.[1] Subsequent security alerts, including by the Australian Cyber Security Centre (**ACSC**), confirm that targeted cyber campaigns continue to occur at a global level and affect Australian organisations.[2]

Multiple levels of government in Australia recognise that cyber security is a key priority for critical infrastructure. Most recently the Australian Energy Sector Cyber Security Framework (**AESCSF**) was developed. The framework helps drive the cyber resilience of individual market participants and the energy sector more broadly, through providing a consistent means to assess and uplift cyber security maturity. Whilst utilising the AESCSF is currently voluntary, we performed a self-assessment as have the majority of other distributors and market participants. The Australian Energy Market Operator (**AEMO**) reports that the initial response rate in 2018 exceeded 85% market coverage for each sub-sector in the National Energy Market (**NEM**).[3]

Cyber security is also a key priority internally, ranking as one our top 10 items on our risk register, and as a result this issue is regularly presented on to our Risk Audit Committee. In addition we have commissioned an external cyber security strategic review which provided a series of recommendations (see attachment CP ATT047 - PWC - Cyber strategy review - Nov19- Confidential).

We have identified a need to invest in expanding the scope and coverage of our cyber security capability to enable us to be:

- **Safe & Dependable**: support the continued safe, reliable, and secure delivery of electricity and the protection of customers' personal information in a threat landscape with more frequent and sophisticated cyber-attacks targeting the energy sector globally and in Australia.
- **Flexible**: provide foundational cyber security services that are flexible and also allow us to maximise opportunities presented by an increasingly digitally-interdependent ecosystem, including through separate initiatives such as solar enablement and a flexible grid.
- **Affordable**: adopt balanced investment in cyber security, which avoids both over and under investment. Under investment would lead to high costs of unplanned recovery and remediation efforts – including potential fines – resulting from a major/significant cyber incident.

---

1 United States DHS, *Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, 25 February 2016 (CP ATT190).

2 Australian Government – Australian Signals Directorate – Australian Cyber Security Centre, *Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors*, 17 April 2018 (CP ATT192).

3 Australian Energy Market Operator Limited, *2018 Cyber Security Preparedness Report*, December 2018 (CP ATT186).

We assessed cyber security drivers and identified initiatives required to meet these drivers. We took a risk-balanced view of corporate IT and industrial OT security, and informed by our AESCSF self-assessment have identified areas where we believe we need to rebalance previous investments and insights.

We developed and compared four options (including the option to do nothing), which progressively expanded the coverage of our security capabilities. For each option, we forecast the capital expenditure and undertook risk monetisation to value the risks. Table 1 summarises the outcome of our options analysis.

Table 1 Options Analysis Summary, $m 2021

Option	Description	Cost	Risk
0	Do Nothing - do not invest in maintaining cyber security capabilities	0.0	183.1
1	Maintain Currency – maintain existing cyber security capabilities as is	19.4	58.6
2	Optimise Effectiveness – build on Option 1 by optimising the effectiveness of existing cyber security capabilities by increasing coverage	27.5	29.3
3	Expand Analytics Capability – build on Option 2 by expanding our cyber security monitoring and behavioural analytics capabilities	39.4	15.5

Source: CitiPower

We recommend option 2, which provides a balance between cost and risk and aligns with the three pillars of safe and dependable, flexible and affordable.

The first two options– doing nothing, and maintaining currency with no further uplift – are not recommended due to the level of risk to our IT systems and network operations. These options detract from our ability to ensure a safe and dependable supply of electricity to our customers, and consequently introduce an unacceptable level of risk to the business, our customers, and the community more broadly.

Option 3 – involving expanding our security monitoring and behavioural analytics capabilities – is not recommended as our analysis shows it does not provide sufficient benefits, in terms of risk reduction, given the significant additional investment required.

2 Background

2.1 Securing the supply of electricity to customers

We are responsible for the safe and reliable delivery of electricity to over 1.2 million homes and businesses across our distribution network. We are part of Australia's critical infrastructure and deliver power to services that are essential for everyday life such as manufacturing, transport, communications, health, banking, and finance. A disruption to the supply of electricity will have serious implications for business, government, and the community.

The safe operation and control of the electrical network relies on IT systems and infrastructure. Distributors operate the grid from network control centres, using a range of telecommunications technologies, including fibre-optic cables and mobile networks. Because of this reliance on technology, IT security and the resilience of the electricity distribution network are inherently linked. For this reason cyber security is one of Australia's top national security priorities,[4] and the Australian government and industry regulators are increasingly focusing on our efforts to secure the critical infrastructure we operate (described in further detail below).

We take cyber security seriously and our cyber security program aligns to section 6.5.6(a)(iii) of the National Electricity Rules (**the Rules**), which state that a distributor must maintain the quality, reliability, and security of supply of standard control services. Cyber security forms part of the top five risks in our enterprise risk register, which are monitored by our Audit and Risk Committee and is discussed at each meeting of our board of directors. We have made considerable investments in cyber security – including through people, processes, and tools – and the initiatives outlined in this business case support the security of the network, its reliability, and performance through the prevention, detection, and timely response to cyber security breaches that may adversely affect our ability as a distributor to supply the electricity that our customers depend on.

2.2 Evolving cyber threat landscape

Cyber threats against Industrial Control Systems (**ICS**) and critical infrastructure continue to increase in intensity, frequency, and complexity. **WEF** Global Risks Report 2019 includes cyber-attacks in the top five global risks by likelihood over a 10-year horizon, noting that over the past two years the position of cyber-risks has been consolidating in the 'high-impact, high-likelihood quadrant of the Global Risks Landscape'.[5]

Cyber-attacks carried out against critical infrastructure have become increasingly sophisticated over the past decade, with real-world impacts on the delivery of critical services and utilities:

- Remote cyber intrusions of three regional electric power distributors in Ukraine resulted in unscheduled outages impacting approximately 225,000 customers in December 2015.[6] This is the first publicly-acknowledged successful cyber-attack on a country's electrical system.
- The US Department of Homeland Security (**DHS**) and Federal Bureau of Investigation (**FBI**) jointly published an alert in March 2018, detailing cyber activities targeting US energy and critical infrastructure sectors, which they attributed to the Russian government.[7] While these are not known to have resulted in destructive activities, they confirm targeted cyber intrusion and the collection of information related to ICS – including evidence that cyber-attackers had accessed systems in the victim's operational technology

---

4 Australian Government – Department of Home Affairs, *Cyber Security Strategy*, accessed 20 August 2018 (CP ATT188).

5 World Economic Forum, *The Global Risks Report 2019* (CP ATT197).

6 United States DHS, *Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, 25 February 2016 (CP ATT190).

7 United States DHS, *Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, 15 March 2018 (CP ATT190).

environment. The ACSC confirmed that Australian organisations were targeted by a global campaign that the US DHS, US FBI, and UK National Cyber Security Centre (**NCSC**) jointly published an alert on in April 2018.[8] This detailed cyber activities are targeting network and security infrastructure devices that underpin most corporate networks – including routers, switches, firewalls, and network-based intrusion detection systems.[9] Critical infrastructure providers were named as one of the primary targets of this attack.

Although there have not been any publicly-disclosed successful cyber-attacks on the Australian energy sector, the ACSC's confirmation (detailed above) that Australian organisations are targeted by global cyber campaigns reinforces the relevance of considering the potential impacts of the global cyber threat landscape to the Australian communities and businesses that rely on a secure supply of electricity. In addition, these examples, supported by official alerts from reputable agencies, validate the observation that cyber-attacks pose risks to critical infrastructure and that a successful cyber-attack on critical infrastructure have the potential to result in devastating spill-over effects.

2.3 Digitally interdependent energy ecosystem

Whilst the physical layer of the energy ecosystem – the transmission and distribution infrastructure connecting generators and customers – is well understood, the increasing digitalisation of the grid is introducing new complexities and interdependencies.[10] IT and OT continue to converge, which increases the digitisation of assets in the field, and the digitalisation of energy distribution more broadly. See CP APP01 - Stakeholder engagement - Jan2020 - Public for a snapshot of our stakeholders' views of our shared energy future, including digitally-underpinned capabilities such as customer access to near real-time data on their energy use and smart meter readings every five minutes.

We have also proposed (through a separate business case) digital network initiatives that will introduce a step change in digital interdependence. These initiatives have a significant digital underpinning, through near real-time data and analytics that support network visibility, as well as operations technology, interfaces, and network automation that support network management. While the digital network business case is separate and designed to stand alone, the security capabilities supported in this document are a shared foundational service, considering the evolving nature of the ecosystem.

2.4 Cyber security focus for the Australian energy sector

Multiple levels of government in Australia have recognised the growing importance of cyber security in the protection of Australia's critical infrastructure and the increase in cyber threats. They have identified it as a key priority for increased attention and investment (detailed further in Appendix B) and the AEMO in conjunction with partners from industry and government developed a tailored framework called the AESCSF, having recognised the national importance of protecting Australia's energy sector against cyber threats.[11]

The AESCSF helps drive the cyber resilience of individual market participants and the energy sector more broadly by providing a consistent means by which to assess and uplift cyber security across 11 domains by using three

---

8 Australian Government – Australian Signals Directorate – Australian Cyber Security Centre, *Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors*, 17 April 2018 (CP ATT192).

9 United States DHS, *Alert (TA18-106A): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, 16 April 2018 (CP ATT190).

10 World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards* (CP ATT196).

11 Australian Energy Market Operator Limited, *Cyber security*, accessed 12 March 2019: https://www.aemo.com.au/Electricity/National-Electricity-Market-NEM/Cyber-Security.

maturity levels: MIL-1 to MIL-3 in order of increasing maturity. Utilising the AESCSF is currently voluntary, but the majority of distributors and market participants' self-assessments conducted in 2018 and AEMO reports that the initial response rate in 2018 exceeded 85% market coverage for each sub-sector in the NEM.[12]

2.5 Other regulatory drivers for cyber security

In addition to regulatory drivers specific to the Australian energy sector, we also store and process personal information of customers and are subject to data and privacy protection regulation. The Australian Privacy Act 1988 (Cth) defines the Australian Privacy Principles (APP) that outline how 'APP entities' – a definition that includes Australian private sector organisations with an annual turnover of more than $3 million – must handle, use, and manage personal information.[13]

One of these principles is APP 11 – security of personal information, which requires APP entities to take reasonable steps to protect personal information they hold. Guidelines issued by the Office of Australian Information Commissioner (**OAIC**) provide further clarification that these reasonable steps include implementing ICT security strategies.[14,15] Subsequently, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) established a data breach notification scheme in Australia, which requires APP entities to notify affected individuals and the OAIC of certain data breaches.[16]

2.6 Internal prioritisation of cyber security

Cyber security is also a key priority internally, ranking as one our top 10 items on our risk register, and as a result this issue is regularly presented on to our Risk Audit Committee.

---

12 Australian Energy Market Operator Limited, *2018 Cyber Security Preparedness Report*, December 2018, accessed 27 March 2019 (CP ATT186).

13 Australian Government – Office of the Australian Information Commissioner, *Australian Privacy Principles*, accessed 19 March 2019: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles.

14 Australian Government – Office of the Australian Information Commissioner, *Chapter 11: APP 11 – Security of personal information version 1.1*, March 2015 (CP ATT209).

15 Australian Government – Office of the Australian Information Commissioner, *Guide to securing personal information*, June 2018 (CP ATT189).

16 Australian Government – Office of the Australian Information Commissioner, *Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, February 2018 (CP ATT187).

Figure 1 Risk Audit Committee Snapshot of Top Risks

Ref.	Risk Title	Risk Description	Inherent Risk Rating	Residual Risk Rating	Control Assessment
1	**Catastrophic bushfire caused by Company activities**	Catastrophic bushfire caused by Company assets and/or by employees or contractors in carrying out work for the Company	Extreme	High	Satisfactory
2	**Health and Safety Incident**	Serious injury or fatality to contractor/ employee or member of public due to Companies activities or workplace hazards	Extreme	High	Satisfactory
3	**Injury or damage to third party caused by Network Asset or Operations**	Injury or damage to third parties caused by Network Assets or Operations	Extreme	High	Satisfactory
4	**Cyber risk**	Unauthorised or malicious changes to our hardware, software or data that could impact system integrity, availability or confidentiality of information.	Extreme	High	Satisfactory
5	**Sabotage or vandalism of Network Assets**	Deliberate sabotage, theft or vandalism of network assets- including environmental damage arising from such activity	High	Medium	Satisfactory

Source: CitiPower

In addition we have commissioned an external cyber security strategic review which provided a series of recommendations (see attachment CP ATT047 - PWC - Cyber strategy review - Nov19- Confidential).

3 Identified need

We need to invest in uplifting our cyber security capability to enable us to support the three pillars that reflect the views and preferences of our stakeholders:

- **Safe & dependable**: support the continued safe, reliable, and secure delivery of electricity, and the protection of customers' personal information in a threat landscape with more frequent and sophisticated cyber-attacks targeting the energy sector globally and in Australia.
- **Flexible**: provide foundational cyber security services that are flexible and also allow us to maximise opportunities presented by an increasingly digitally-interdependent ecosystem, including through separate initiatives such as a flexible grid.
- **Affordable**: adopt a balanced investment in cyber security, which also avoids the high costs of unplanned recovery and remediation efforts – including potential fines – that will be required in the event of a major/significant cyber incident.

3.1 Current state

Cyber security is a key priority for us and is one of the top five risks in our enterprise risk register. As such, cyber security is monitored continuously by our Audit and Risk Committee and is discussed at every meeting of our board of directors. Capabilities we implemented through investments in cyber security over the past five years have successfully detected and protected our IT and OT infrastructure and customers' personal information against a variety of cyber-attacks.

As a result, we have not experienced major/significant impacts from a cyber security incident in the past five years. We also participated in the voluntary self-assessment exercise using the AESCSF, where we score 1.8 and ranked eighth in the NEM-wide rankings and third amongst distributors. Overall, we believe that our cyber security maturity is a positive indication of the investments we have made to date.

However – and as detailed in the background section of this document – the cyber security threat landscape is rapidly evolving and will continue to do so, with threats becoming more sophisticated and the energy ecosystem becoming increasingly digitally interdependent. While our current cyber security capabilities are effective today, we need to continue investing to manage future threats.

3.2 Desired future state

Our desired future state is a cyber security capability that continues to ensure we have a safe and dependable network, can flexibly adapt, and remains affordable to customers. To achieve these high-level objectives, we have identified key initiatives that comprise our cyber security investment program.

These initiatives are:

- Aligned with the five core functions of the National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**), which we use to structure our cyber security program more broadly.
- Informed by our self-assessment using the AESCSF and an acknowledgement that, although AESCSF maturity target states have not been formally communicated (or mandated at this time), we need investments to support our progression towards a higher maturity level given the number of critical and commercial customers we supply electricity to vis a vis the AESCSF guidance on criticality bands by market subsector. Notably, should the AESCSF highest maturity level (MIL-3) be mandated we would need to assess the extent of further uplifts to our cyber security required to ensure compliance with the higher level of maturity.

- Guided by recommended practices including the ACSC's 'Essential Eight' strategies to mitigate cyber security incidents[17] and the North American Electric Reliability Corporation (**NERC**) Critical Infrastructure Protection (**CIP**) standards[18].
- Intended to achieve a security capability that, when adjusted for risk, is balanced between corporate IT and industrial OT.

Figure 2 Core functions of the NIST CSF

Source: National Institute of Standards and Technology

3.3 Key initiatives

To achieve our desired future state, we propose the following key initiatives as part of our cyber security investment program for 2021–2026:

- **Identify** – initiatives aligned with the 'Identify' NIST CSF function will help broaden our ability to proactively assess, manage, and govern cyber risks. These will support the maintenance or uplift in maturity across seven AESCSF domains.
- **Protect** – initiatives aligned with the 'Protect' NIST CSF function will provide the core technical capability to secure customer data and protect critical infrastructure against cyber threats, and is where most of our proposed investment is aligned. These initiatives will support the uplift in maturity across three AESCSF domains.
- **Detect** – initiatives aligned with the 'Detect' NIST CSF function will enable us to uplift our ability to detect anomalous behaviour and the presence of advanced persistent threats. These will support the uplift in maturity across two AESCSF domains.

Respond – the initiative aligned with the 'Respond' NIST CSF function will enable us to improve our ability to assess the impact of incidents and will support other functions by allowing us to improve protection and

[17] Australian Government – Australian Signals Directorate – Australian Cyber Security Centre, *ACSC Protect: Essential Eight Explained*, January 2019 (CP ATT185).

[18] North American Electric Reliability Corporation, CIP Standards, accessed 27 March 2019: https://www.nerc.com/pa/Stand/pages/cipstandards.aspx.

detection, using lessons learnt from the incident analysis, as well as serving as an input to threat intelligence information sharing.

4 Options analysis

4.1 Approach

Assess

We assessed cyber security drivers and needs with the help of internal SMEs and external cyber security consultants, anchored on the following (detailed in the background section above):

- core principles of our responsibility under the Rules as an electricity distributor that is classified as critical national infrastructure
- external factors through the cyber security landscape, trends, and emerging threats, both in general terms as well as relating to the Australian energy sector specifically
- internal strengths and weaknesses, including consideration of the results of our 2018 cyber security maturity self-assessment using the AESCSF.

Identify

We identified initiatives that will address our cyber security needs and expand the scope and coverage of our cyber security capabilities during the 2021–2026 regulatory period. We looked across the five NIST CSF functions referred to in the background section of this document, as well as the 23 categories that underpin these functions. The objective of this anchoring was to achieve a balanced investment across the four relevant functions from an investment perspective – noting that the fifth function of 'recover' does not apply to this business case as this domain relates exclusively to processes and procedures that are already in place. We also took a risk-balanced view of both corporate IT and industrial OT security, which was further informed by areas where we believe we need to rebalance previous investments, as well as insights from our AESCSF self-assessment.

Compare

We developed and compared three options (in addition to the option to do nothing), which progressively build on each other to expand the coverage of our security capabilities. We took this approach to developing and comparing options as it allowed us to maintain a risk-balanced coverage across NIST CSF functions as well as IT and OT.

Given the timeframe involved for the 2021–2026 regulatory period and the rate of change in the cyber security industry (and specifically with the evolution of cyber security tools), it was not practical to compare specific products and it was necessary for our analysis to be abstracted at the security capability level.

Recommend

We selected and recommend option 2, providing further detail on the justification in the recommendation section of this document.

Estimate and roadmap

We estimated the recommended option using historical project costs, with adjustments for additional scope where required. Estimates were produced in terms of labour, contracts and material costs, with labour rates being based on a blended external IT labour rate provided by PwC.[19]

We also developed a high-level roadmap over the period 2021–2026 using the license expiry or end-of-life date of the equivalent capability currently in place to allow us to maximise investments already made in these current capabilities. Due to the sensitive nature of cyber security and specifically of disclosing end-of-life dates of security capabilities, this information has been excluded from this document.

4.2 Summary

We considered four options for this cyber security business case following the approach outlined above. These options are described as follows:

- Option 0 involves not investing in cyber security capabilities, which will result in continuing to operate security services on a 'best effort' basis despite hardware and software reaching end-of-life and ceasing to receive vendor support and security updates.
- Option 1 involves maintaining existing security capabilities as is, without further investment into uplifting, developing, or expanding them.
- Option 2 optimises the effectiveness of existing security capabilities through an increase in scope of their coverage. In a few cases where the existing security capabilities do not provide adequate coverage despite an increase in scope, additional initiatives have been included to address these needs
- Option 3 expands our security monitoring and behavioural analytics capabilities, in addition to the scope of option 2.

Table 2 summarise the costs and risks of each option over the regulatory period 2021–2026.

Table 2 Options summary, $m June 2021

Option	Description	Cost	Risk
0	Do Nothing - do not invest in maintaining cyber security capabilities	0.0	183.1
1	Maintain Currency – maintain existing cyber security capabilities as is	19.4	58.6
2	Optimise Effectiveness – build on Option 1 by optimising the effectiveness of existing cyber security capabilities by increasing coverage	27.5	29.3
3	Expand Analytics Capability – build on Option 2 by expanding our cyber security monitoring and behavioural analytics capabilities	39.4	15.5

Source: CitiPower

[19] See UE MOD 12.02 - Quoted services labour rate - Jan2020 - Public.

4.3 Option 0 – do nothing

The 'do nothing' option involves not investing in cyber security capabilities. This will result in continuing to operate security services on a 'best effort' basis despite hardware and software reaching end-of-life and ceasing to receive vendor support and security updates. As demonstrated by the risk monetisation outcome, this option introduces an unacceptable level of risk to the business, our customers, and the community more broadly, so doing nothing is not a viable option. Appendix A provides more information on the risks of not maintaining our cyber security capabilities.

Table 3 provides further detail to the key disadvantages of option 0.

Table 3 Advantages and disadvantages of option 0

Category	Advantages	Disadvantages
Safe & Dependable		Reliance on unsupported (end-of-life) security capabilities during the period 2021–2026 will significantly reduce the organisation's ability to protect against and detect cyber-attacks, increasing the likelihood of a major/significant cyber security incident.
		Increased likelihood that a major/significant cyber security incident may result in a failure to deliver a safe and dependable supply of electricity to customers, breaching of section 6.5.6(a)(iii) of the Rules.
		Increased likelihood of a data breach involving customers' personal information, which will require mandatory notification and potential fines under the Privacy Act 1988.
Flexible		Unsupported security capabilities will not address new or emerging security threats.
Affordable	No capital expenditure for cyber security.	Significant costs will be incurred both as a direct consequence of – and in order to respond to and remediate – security breaches, including potential fines.

Source: CitiPower

4.4 Option 1 – maintain currency

We have invested in cyber security capabilities that have been effective so far. This option involves maintaining these existing capabilities as is, without further investment in uplifting, developing, or expanding them.

The main advantage of this option is reduced capital expenditure, which would be limited to:

- refreshing hardware to avoid the risks related to running security software on unsupported or inadequate hardware
- implementing 'major version' software upgrades to avoid the risks related to using unsupported, deprecated, or end-of-life software

- renewing or purchasing software licenses to remain within support periods (i.e. not operate end-of-life or unsupported versions of software) and compliant with our obligations.

However, whilst this option avoids the risks resulting directly from operating unsupported or end-of-life components, it does not address the following:

- the cyber threat landscape is evolving rapidly and current-generation capabilities are unlikely to detect and protect against emerging threats, as discussed in the background section of this document
- the energy ecosystem is becoming increasingly digitally interdependent and while our other proposed initiatives (e.g. flexible grid) are designed to stand alone, cyber security capabilities are a shared foundational service. Current-generation security capabilities are unlikely to be able to provide the coverage and integration required for these proposed initiatives, resulting in a net reduction of our ability to protect against and detect cyber-attacks
- this level of investment does not provide the support required to enable our progression towards the highest maturity level (MIL-3) of the AESCSF.

Consequently, whilst the level of risk introduced by this option is substantially less than for option 0, it remains an unacceptable level of risk and is not a viable option. Refer to the Cyber security risk monetisation model for more detail on the risk of option 1.

Table 4 provides further detail to the key disadvantages of option 1.

Table 4 Advantages and disadvantages of option 1

Category	Advantages	Disadvantages
Safe & Dependable		Reliance on current security capabilities maintained as is with no further uplift during the period 2021–2026 increases the likelihood of a major/significant cyber security incident as these capabilities will not detect or protect against emerging threats, resulting in a net reduction in our ability to protect against and detect cyber-attacks.
		Increased likelihood that a major/significant cyber security incident may result in a failure to deliver a safe and dependable supply of electricity to customers, breaching of section 6.5.6(a)(iii) of the Rules.
		Increased likelihood of a data breach involving customers' personal information, which will require mandatory notification and potential fines under the Privacy Act 1988.
Flexible		Security capabilities maintained as is are unlikely to be able to adequately address new or emerging security threats.
		Security capabilities maintained as is will not be able to be providing the foundational cyber security services required by planned initiatives (e.g. solar enablement and flexible grid).
Affordable	Lower capital expenditure to maintain existing security capabilities as is.	Significant costs will be incurred both as a direct consequence of – and in order to respond to and remediate – security breaches, including potential fines.

Source: CitiPower

4.5 Option 2 – optimise effectiveness

This option optimises the effectiveness of the security control landscape holistically by maintaining currency (as outlined in the previous option) and increasing the scope or coverage. Key initiatives recommended in this option include:

- **Identify** – three key initiatives that will help broaden our ability to proactively identify vulnerabilities, manage risks and track remediation activities, and consume and share threat intelligence information with trusted partners.
- **Protect** – 17 key initiatives that support our ability to more effectively and efficiently manage human and machine identities, control access to sensitive systems, secure customer data, and protect critical infrastructure.
- **Detect** – eight key initiatives that will enable us to uplift our ability to detect anomalous behaviour and the presence of advanced persistent threats, through capabilities that allow us to collect and analyse more in-depth security-related data across a broader section of our IT and OT networks and devices.

- **Respond** – one key initiative that will enable us to improve our ability to assess the impact of incidents.

Most of these initiatives uplift existing capabilities, including some that were implemented in the 2016–2020 regulatory period, by providing additional investment to enable these capabilities to operate to their full potential. However, our AESCSF self-assessment allowed us to identify areas requiring additional investment, resulting in us introducing some new initiatives to supplement the capability of some of our current tools.

Notably, should the AESCSF highest maturity level (MIL-3) be mandated we would need to assess the extent of further uplifts to our cyber security required to ensure compliance with the higher level of maturity.

Table 5 provides further detail to the key advantages and disadvantages of option 2.

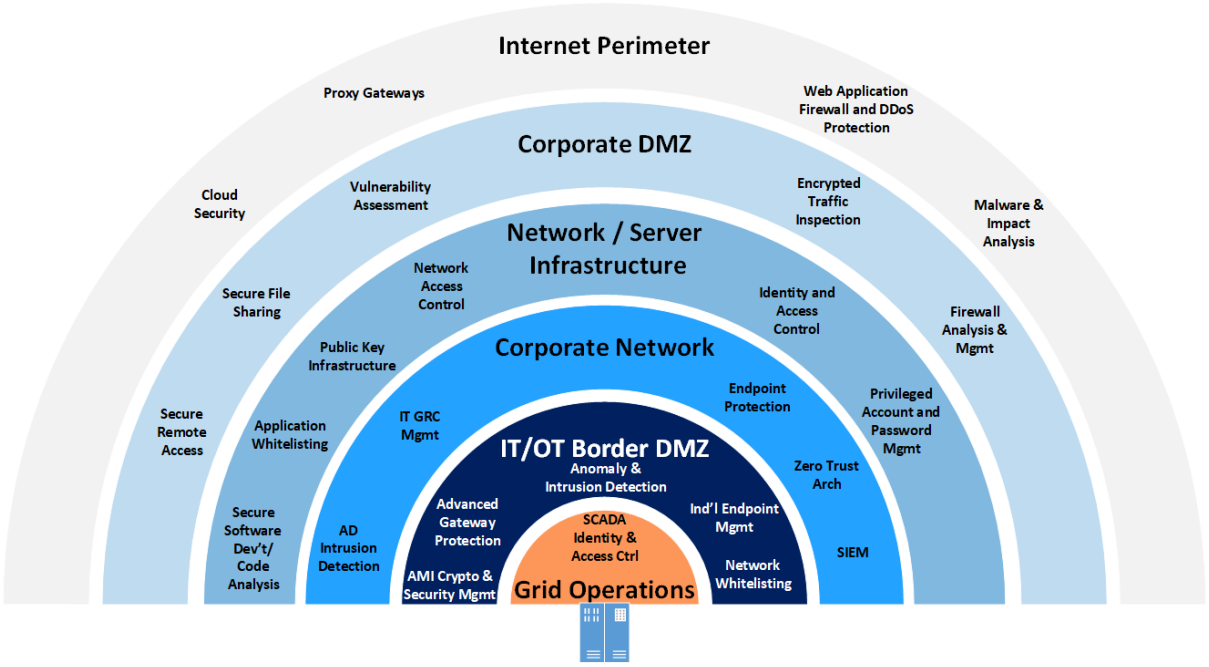
Table 5 Advantages and disadvantages of option 2

Category	Advantages	Disadvantages
Safe & Dependable	Balanced investment in cyber security to enable the delivery of a safe and dependable supply of electricity to customers by: • reducing the likelihood that a cyber security incident occurs • increasing our ability to detect and respond to cyber security breaches in a timely manner, before they result in major incident.	
	Balanced investment in cyber security to protect the confidentiality and integrity of customers' personal information and avoid the impacts of mandatory notification and fines under the Privacy Act 1988 by: • reducing the likelihood of a data breach involving customers' personal information • increasing our ability to detect and respond to data breaches in a timely manner so that their negative impacts may be minimised.	
Flexible	Balanced investment option that includes reasonable provisions to address new or emerging security threats based on an assessment of the cyber security threat landscape and industry trends.	
Affordable	Balanced investment option that maximises previous investments in cyber security capabilities.	Higher capital expenditure for cyber security compared to the two previous options.

Source: CitiPower

The diagram below depicts our defence-in-depth model, with each layer representing both logical and physical layers of our security architecture, and where key controls that form part of the recommended option are placed.

Figure 3 Defence-in-Depth Security Architecture



Source: CitiPower & Powercor

4.6 Option 3 – expand analytics capability

This option expands our security monitoring and behavioural analytics capability. In addition to the full scope of option 2, this option also includes two key initiatives aligned with the 'Detect' function:

- enhance cyber security monitoring through the implementation of a 'single operating view' capability covering both IT and OT security across the organisation
- enhance cyber threat detection through a behavioural analytics capability that identifies abnormal and potentially malicious activities based on a user's role and typical behaviour.

These additional initiatives will further uplift our ability to proactively detect and respond to cyber threats, in particular to address the evolving nature of the tools, tactics, and procedures that cyber-attackers employ and the increasingly complex environment that our cyber security team monitors. However, this option is significantly more expensive than the previous options, due to the nature of these tools.

Table 6 provides further detail to the key advantages and disadvantages of option 3.

Table 6 Advantages and disadvantages of Option 3

Category	Advantages	Disadvantages
Safe & Dependable	Proactive investment in cyber security to enable the delivery of a safe and dependable supply of electricity to customers by: • reducing the likelihood that a cyber security incident occurs • increasing our ability to detect and respond to cyber security breaches in a timely manner, before they result in major incident. Proactive investment in cyber security to protect the confidentiality and integrity of customers' personal information and avoid the impacts of mandatory notification and fines under the Privacy Act 1988 by: • reducing the likelihood of a data breach involving customers' personal information • increasing our ability to detect and respond to data breaches in a timely manner so that their negative impacts may be minimised.	
Flexible	Proactive investment option that includes provisions to address new or emerging security threats based on an assessment of the cyber security threat landscape and industry trends.	
Affordable		Highest capital expenditure for cyber security compared to the other options.

Source: CitiPower

5 Recommendation

We recommend option 2 as this provides a balanced cost-risk investment approach that considers the contribution of cyber security to the pillars that reflect the views and preferences of our stakeholders and the National Electricity Objective (**NEO**):

- **Safe & Dependable**: option 2 supports the continued safe, reliable, and secure delivery of electricity, and the protection of customers' personal information in a threat landscape with more frequent and sophisticated cyber-attacks targeting the energy sector globally and in Australia.
- **Flexible**: option 2 provides foundational cyber security services that are flexible and also allow us to maximise opportunities presented by an increasingly digitally-interdependent ecosystem. These foundational services can also be shared with separate initiatives such as solar enablement and a flexible grid.
- **Affordable**: option 2 reflects a balanced investment in cyber security, which also avoids the high costs of unplanned recovery and remediation efforts – including potential fines – that will be required in the event of a major/significant cyber incident.

We do not recommend the other options for the following reasons:

- Option 0 and option 1 detract from our ability to ensure a safe and dependable supply of electricity to our customers, and consequently introduce unacceptable levels of risk to the business, our customers, and the community more broadly. Therefore, whilst they may be appealing from an affordability perspective, they are not viable options from a risk perspective.
- Option 3 does not provide sufficient additional security benefits given the additional investment, as the existing controls and residual risk are not commensurate to the additional investment required.

Importantly, should the AESCSF highest maturity level (MIL-3) be mandated we would need to assess the extent of further uplifts to our cyber security required to ensure compliance with the higher level of maturity.

Table 7 summarises the expenditure profile for option 2 in the 2021–2026 regulatory period.

Table 7 Recommended option: expenditure profile, $m June 2021

Expenditure forecast	2021/22	2022/23	2023/24	2024/25	2025/26	Total
CitiPower	1.6	1.7	1.8	1.7	1.4	8.3
Powercor	3.8	3.9	4.2	4.1	3.2	19.3
Total	**5.5**	**5.6**	**6.0**	**5.8**	**4.6**	**27.5**

Source: CitiPower

Table 8 below provides the expenditure forecasts for option 2 by recurrent and non-recurrent categories. The recurrent expenditure forecast reflects the cost to maintain our current IT cyber security capabilities and the non-recurrent expenditure forecast reflects the cost to uplift our cyber security capabilities.

Table 8 Recommended option: expenditure profile, $m June 2021

Expenditure forecast	2021/22	2022/23	2023/24	2024/25	2025/26	Total
Recurrent	3.8	3.9	4.2	4.1	3.2	19.4
Non-recurrent	1.6	1.7	1.8	1.7	1.4	8.2
Total	**5.5**	**5.6**	**6.0**	**5.8**	**4.6**	**27.5**

Source: CitiPower

A IT Risk monetisation

Table 9 IT Risk Monetisation Framework

Risk Category	Risk Type	Description of Risk
IT Risks	Outage	Increased likelihood of an outage of the security capability itself (e.g. instability due to unsupported hardware or software). Increased likelihood of an outage of other corporate IT infrastructure due to ineffective operations of the security capability meant to protect them (e.g. a denial of service attack that is not effectively blocked by the web application firewall).
	Data Breach	Increased likelihood of a data breach due to ineffective operations of the security capability meant to protect against this at a particular layer. Reduced ability to detect a data breach in a timely manner. Increased effort required to identify and remedy the cause of the data breach.
	Malicious Control	Increased likelihood that an external threat actor or malicious insider is able to gain malicious control of the: • operational technology interfaces that control the electricity distribution network • enterprise applications • corporate network • staff and contractor devices.
	System Sustainability	Increased technical debt as workarounds are required to compensate for legacy cyber security services, notably when they reach their end-of-life dates and cease to receive support.
	Suitability	Decreased ability to provide adequate protection for corporate IT and industrial OT infrastructure against cyber security threats as security requirements evolve.
Business Risks	Reliability Impact	Malicious control of operational technology interfaces that control the electricity distribution network may result in the disruption of power supply to our customers.

Risk Category	Risk Type	Description of Risk
	Compliance Risk	The Secretary of the Department of Home Affairs may issue directions to mitigate national security risks under the Security of Critical Infrastructure Act 2018 (Cth). • The Australian Energy Regulator may seek civil penalties or apply for civil penalty orders for unplanned power outages that result in a breach of obligations under the Rules. • The Australian Information Commissioner may seek civil penalties or apply for civil penalty orders of up to $1.7m for data breaches under the Privacy Act 1988.
	Customer Experience Risk	IT risks materialising as a result of a cyber security incident – specifically outages, data breaches involving customer information, and malicious control of infrastructure – will adversely impact customer interactions.
	Bushfire Risk	Outages of the operational technology interfaces that provide visibility of the network may increase bushfire risk by preventing operators from making accurate and timely decisions. Malicious control of operational technology interfaces that control the electricity distribution network may increase bushfire risk, for example by reenergising sections of the network that has been shut down preventively to decrease risk.
	Safety Risk	Malicious control of operational technology interfaces that control the electricity distribution network may result in safety and health consequences to workers, consumers, and the public. For example: • re-energising a section of the network that is expected to be de-energised for planned maintenance works • disruption of power to customers who rely on life support equipment.

Risk Category	Risk Type	Description of Risk
	Financial Loss	Malicious control of enterprise applications may allow threat actors to tamper with the integrity of information in ways that result in direct financial consequence not otherwise taken into account in any of the above areas of consequence. For example, this may involve modifying data or application behaviour to alter meter reading values, resulting in a loss of revenue.

Source: CitiPower

B Cyber Security Focus for Australian Energy Sector

Multiple levels of government in Australia have recognised the importance of cyber security in the protection of Australia's critical infrastructure, and have identified it as a key priority for increased attention and investment:

- The Victorian Government released its Critical Infrastructure Resilience Strategy in 2016, which acknowledges the cyber dependency of critical infrastructure and directs all Victorian critical infrastructure owners and operators to prepare for cyber-attacks as they do other emergency risks.[20]
- Victoria's Critical Infrastructure All Sectors Resilience Report 2017 includes cyber security as one of 15 key risks to the energy sector in Victoria.[21] This aligns with the ACSC Threat Report 2017, which notes that high-value targets like critical infrastructure would be the likely target of a cyber-attack against Australia with the energy sector ranking within the top four most-targeted industries.
- The Australian Security of Critical Infrastructure Act 2018 (Cth) provides the Secretary of the Department of Home Affairs with powers to gather information and issue directions for the owner or operator of a critical infrastructure asset to mitigate national security risks.[22]
- The 2017 Independent review into the future security of the National Electricity Market: Blueprint for the future – also referred to as the 'Finkel Review' – recognises that cyber vulnerabilities of electricity market participants are increasing due to the growing integration of information and communication technology and connectivity with open networks, and recommends that cyber security preparedness be assessed and reported on annually.[23]

Having recognised the national importance of protecting Australia's energy sector against cyber threats – and in response to recommendation 2.10 of the Finkel Review – the AEMO in conjunction with partners from industry and government developed a tailored framework called the AESCSF.[24] The AESCSF helps drive the cyber resilience of individual market participants and the energy sector more broadly by providing a consistent means by which to assess and uplift cyber security across 11 domains using three maturity levels: MIL-1 to MIL-3 in order of increasing maturity.

---

20 State Government of Victoria – Emergency Management Victoria, Critical Infrastructure Resilience Strategy, September 2016 (CP ATT193).

21 State Government of Victoria – Emergency Management Victoria, Victoria's Critical Infrastructure All Sectors Resilience Report 2017, November 2017 (CP ATT194).

22 Australian Government – Department of Home Affairs, Security of Critical Infrastructure Act 2018.

23 Commonwealth of Australia, Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future, 2017 (CP ATT191).

24 Australian Energy Market Operator Limited, Cyber security, accessed 12 March 2019: https://www.aemo.com.au/Electricity/National-Electricity-Market-NEM/Cyber-Security.