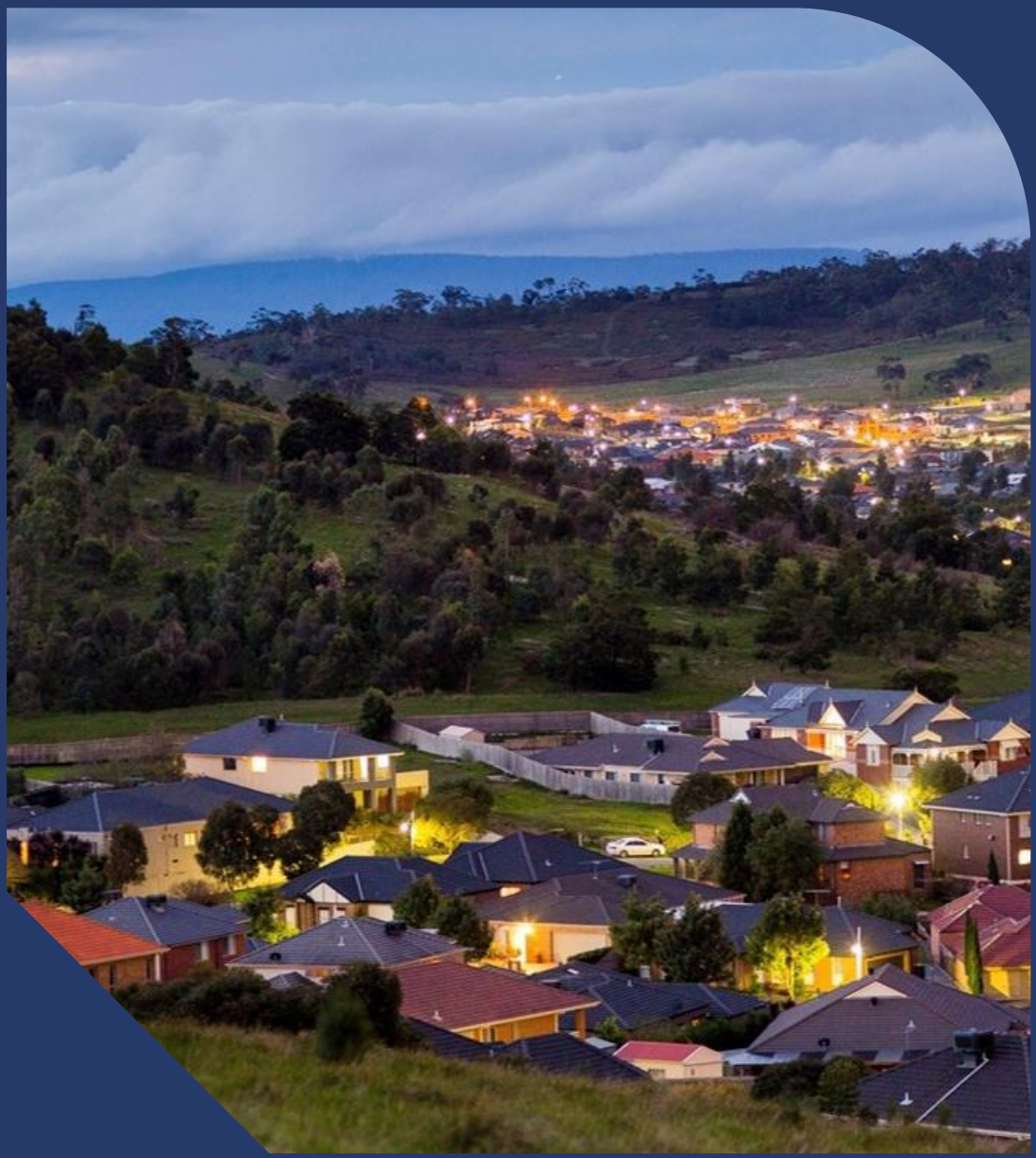
AusNet

Electricity Distribution Price Review FY2027 to FY2031 (EDPR 2027-31)

Business case: Cyber Security

Date: January 2025



AusNet

Table of contents

Document history

DATE	VERSION	COMMENT
28/10/2024	V1.0	Initial draft business case for review
02/12/2024	V2.0	Revised business case incorporating SME review
15/01/2025	V3.0	Final business case document

Related documents

DOCUMENT	VERSION	AUTHOR
Technology Strategy and Investment Plan	V3.0	AusNet Services
AusNet EDPR 2027-31 Digital Program NPV model	V3.0	AusNet Services

Approvals

POSITION	DATE
Digital & Technology – Strategy, Regulatory and Partner Management	January 2025
Digital & Technology – Architecture	January 2025
Digital & Technology – Cyber Security	January 2025
Distribution – Strategy and Regulation	January 2025

1. Executive summary

AusNet has a complex and integrated suite of technology systems, applications and infrastructure that enable us to deliver an affordable and reliable electricity distribution network service to our customers. Keeping our digital assets secure from cyber threats is fundamental, given the potential for widescale disruption of our electricity services resulting from a successful cyber compromise. Such a scenario would significantly disrupt the lives of our customers, put vulnerable customers at risk, and have widespread economic impacts. A prolonged outage could also give rise to consequential failure of other essential services such as telecommunications, transportation, banking, healthcare, water and sewage; all which rely on electricity.

Cyber security threats have intensified over the past 5 years with a spate of major attacks on businesses in Australia such as Optus and Medibank. While this reflects the evolution of threat actor capabilities, the threats have also intensified as a result of geo-political instability that is fuelling the risk of state-sponsored sabotage. The enhanced threat level coincides with increasing digitalisation and automation of electricity networks, as well as the integration of third-party renewables and customer energy resources with our network.

As detailed in the *Annual Cyber Threat Report 2023-2024 published by the Australian Signals Directorate (ASD)*[1] and the *2024 National Defence Strategy*, Australia faces the most complex and challenging strategic environment since the Second World War, and these challenges extend to the cyber threat landscape where in the event of a major deterioration in the strategic environment, Australia could be the target of significant disruptive cyber activities. While advancements in emerging technologies offer significant social and economic benefits, they also improve the capabilities of malicious cyber threat actors who continue to target Australian businesses and infrastructure. State-sponsored cyber threat actors persistently target Australian governments and critical infrastructure with evolving tradecraft. These actors conduct cyber operations in pursuit of geopolitical goals including for espionage, interference and coercion, and in seeking to pre-position for future disruptive cyber attacks.

In additional to this, cyber threat actors and criminals are continuously evolving and adapting to capitalise on new opportunities and advancements in technologies, such as artificial intelligence which reduces the level of sophistication needed for cybercriminals to operate making is easier to compromise organisations and create more disruptive events.

The combination of heightened geopolitical tensions and evolving cyber threat landscape have placed significant pressure on the collective cyber resilience and security of critical infrastructure across Australia. In response, the Australian Government has reaffirmed its commitment by rolling out a comprehensive cybersecurity strategy, allocating funding for its implementation, and enacting multiple legislative reforms. In the series, on November 25, 2024, Parliament passed key legislative changes to bolster national cyber defenses, including amendments to the SOCI Act through the Enhanced Response and Prevention Bill 2024. Aligned to the objective of these reforms, the Australian Energy Market Operator (AEMO) also advanced the Australian Energy Sector Cyber Security Framework (AESCSF) by rolling out version 2. This updated version introduces significant changes designed to align with international standards and address emerging technologies and evolving cyber threats, best suitable for the energy sector to adopt and comply.

AusNet has undertaken significant investment in the 2021-26 period to achieve a Security Profile 2 maturity under the first version of the AESCSF. In the FY2027-31 regulatory period we are proposing distribution network investment of $24.9 million capex, across recurrent and non-recurrent expenditure, to maintain our existing cyber security systems and applications, and uplift cyber capabilities in line with a Security Profile 3 maturity as specified the second version of the AESCSF. In evaluating this recommendation, we considered two options to uplift our cyber capabilities in alignment with the updated AESCSF V2 framework.

- **Option 1** – Uplift our cyber capabilities to achieve the updated SP2 maturity level.
- **Option 2** – Uplift our cyber capabilities to achieve the SP3 maturity level.

We recommend proceeding with **Option 2** since:

- AusNet, as an organisation, is classified as a "High" criticality service provider under the AESCSF, making SP3 the prudent and best practice maturity level for the organisation.

[1] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

- Relative to AusNet's enterprise risk management framework, SP3 sees risks reduced as far as reasonably practical. In contrast, SP2 results in an elevated risk rating, leaving key risks outside of AusNet's risk appetite.
- SP3 allows AusNet to implement the most robust controls to protect data and ensure the resilience and continuity of critical services. In contrast, SP2 leaves AusNet with a higher level of residual risk and less effective controls, increasing the likelihood and impact of cyber incidents compared to the enhanced protection offered by SP3.

While this submission is focused on AusNet distribution, AusNet is accountable for both distribution and transmission in Victoria, and our cyber security controls are designed, implemented and operated at a whole-of-organisation level. A cyber attack impacting our transmission network would impact all electricity customers in Victoria, and potentially place the entire National Electricity Market at risk through cascading impacts. This is reflected in the AESCSF framework that places transmission networks at the highest level of criticality, and it is particularly prudent for AusNet to manage to the highest level of risk. While distribution networks are considered somewhat less critical than transmission networks in the context of the NEM, it would not be feasible to apply a 'lower level' cyber security maturity target for our distribution network given that cyber security systems, digital systems in IT and OT, applications and infrastructure are shared. AusNet's Cost Allocation Methodology provides for fair allocation commensurate to distribution cyber risk profile, with the distribution network forecast to bear only 25% of the total expenditure on shared cyber security expenditure, representing improved value for customers compared to a standalone approach.

Cyber security is not set-and-forget, and as threat actors continue to evolve and innovate, we must continue to evolve and uplift our security practices and our maturity to defend and protect the supply of electricity, our customers and the economy in which we operate.

2. Context

2.1. Background

Digital transformation has enabled AusNet to improve the efficiency of our service delivery and to provide enhanced customer experience. We operate more than 200 digital applications and systems supported by on-premises and cloud-hosted infrastructure. In the next regulatory period, we will be further expanding our digital services to improve our customer experience, network operations capabilities, asset management practices and staff productivity. As we increasingly rely on technology to deliver safe and reliable electricity to our customers, and to run our business efficiently, we must ensure that our digital assets are resilient to cyber threats and operational disruptions.

AusNet takes a risk-averse approach to manage cyber threats and risks by adopting industry best practices, as far as reasonably practicable, to protect our digital assets, energy networks and ultimately our customers. This business case outlines our proposed investments to uplift our cyber capability maturity to meet Security Profile 3 (SP-3) as defined in Version 2 of the Australian Energy Sector Cyber Security Framework (AESCSF).

2.2. Achievements in the current 2021-26 period

AusNet has made notable improvements to the maturity of its cyber security capabilities during the FY2021-26 regulatory period across our business. Consistent with our FY2022-27 Transmission Revenue Reset (TRR) determination, we expect to have achieved Security Profile 2 (SP-2) as defined in version 1 of the AESCSF.

We have focused our investment on the following outcomes:

- Establishing an internal cyber security workforce, defining and communicating cyber security roles and responsibilities across the organisation.
- Implementing a cyber security risk management framework and supporting platform.
- Creating an inventory of Information Technology (IT) and Operational Technology (OT) assets, prioritising assets and defining secure configuration baselines.
- Improving our identity & access management systems and processes, establishing a centralised identity store and implementing multi-factor authentication.
- Enhancing our security threat and vulnerability management capabilities, improving the effectiveness of incident response processes and maturing our security operations function.
- Participating in the wider intelligence sharing community and improving our monitoring and reporting of cyber security threats and risks.
- Embedding cyber security activities in our digital supply chain, including undertaking security assessments of external third-party suppliers.
- Broadening our workforce security awareness and training programs.

As a multi-network business, with predominantly common and shared digital infrastructure, our cyber uplift initiatives apply across our transmission and distribution networks. As a result, cyber security capabilities for our electricity distribution network are also expected to reach an SP-2 level (AESCSF version 1) by the end of the 2021-26 regulatory period.

AusNet's Cost Allocation Methodology (CAM) provides mechanism for fair allocation of investment across our networks to achieve a common outcome, rather they trying to target two discreet risk profiles for distribution and transmission through parallel programs. A key benefit of this approach for our customers is that the distribution network sees a smaller portion of cyber uplift costs to deliver this outcome. As a result, the investment required to reach SP-2 is much lower than our stand-alone distribution network peers. Along with these customer benefits, of greater cyber security at a lower cost, it would also be impractical for AusNet to have separate cyber capabilities for our transmission and distribution networks, given that the underlying technology systems are largely shared.

2.3. Cyber threat landscape

"State-sponsored cyber threats: Growing risks for Australia's critical infrastructure", The Australian Signals Directorate's (ASD) Annual Cyber Threat Report 2023–2024,[2] highlights a rapidly evolving cyber threat landscape, aligning with the challenging strategic environment outlined in the 2024 National Defence Strategy[3] and the 2023-2030 Australian Cyber Security Strategy[4].

The ASD report highlights that state-sponsored cyber operations pose a persistent and increasing threat to Australia, driven by strategic competition in the Indo-Pacific, global conflicts and heightened geopolitical tension. These threat actors target Australian governments, critical infrastructure, businesses, and supply chains for espionage purposes and to establish footholds for launching future disruptive attacks. In February 2024, the ASD, alongside Five Eyes partners, highlighted that Chinese state-sponsored actors are preparing for potential disruptive cyber attacks on US critical infrastructure, with Australia facing similar state-sponsored malicious cyber activity as seen in the US.

Australian data and communications networks, particularly those supporting critical infrastructure assets, are key targets for state-sponsored cyber threat actors seeking to conduct espionage and establish footholds for future attacks. These threat actors pursue sensitive data, intellectual property, and personal information to secure strategic advantages. The exploitation of previously stolen data and persistent vulnerabilities in Australian systems enables ongoing targeting.

Critical infrastructure remains especially attractive to malicious cyber actors due to the essential services it provides to Australian society. The reliance of Australian organisations on intricate networks, complex digital supply chains, and disparate technology management systems expands the attack surface and heightens the risk of exploitation. Disruptions to critical infrastructure could have far-reaching consequences, directly impacting the daily lives of Australians. A prolonged failure in the energy sector for instance could disrupt medical supply chains, food distribution, telecommunications, transport systems, and fuel availability. Additionally, data breaches may expose personal or commercially sensitive information, which can be sold or repurposed for further malicious activity.

2.4. Threats to Operational Technology (OT)

Operational Technology (OT) refers to the systems which monitor and control physical processes in the real world. Within the energy sector, common OT systems include Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS), Outage Management Systems (OMS), Advanced Distribution Management Systems (ADMS), Distributed Energy Resource Management Systems (DERMS) and others. In conjunction with thousands of OT devices deployed in the field (e.g. Human Machine Interfaces (HMIs), Remote Termination Unis (RTUs), etc), these mission-critical OT systems are used to monitor and control the flow of electricity across our energy networks.

OT systems are prime targets for malicious cyber threat actors due to several factors, including:

- Their role in supporting the critical infrastructure which underpins the delivery of essential services.
- Their longer operational lifespans (often spanning decades) and slower rate of change compared to Information Technology (IT) systems, often leading to the existence of unpatched security vulnerabilities.
- Their reliance on legacy insecure communications protocols which do not support security controls such as authentication, encryption and non-repudiation.

Australia's energy transition is driving increased digitisation of OT systems as businesses demand more operational analytics and insights to realise efficiencies and unlock new value streams. To meet this demand, OT systems are becoming increasingly digitised and integrated with organisations' IT systems and external networks. This "IT-OT convergence" offers many business benefits, but also exposes our critical OT systems to additional cyber threats and risks.

Furthermore, new regulations requiring Distribution Network Service Providers (DNSPs) to monitor and control Distributed/Customer Energy Resources (DER/CER) have resulted in the deployment of new OT systems (e.g. Low

[2] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
[3] https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program
[4] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

Voltage DERMS) which need to be able to communicate with external unmanaged DER/CER assets over the public Internet – a paradigm shift which is further expanding the cyber attack surface of our OT environments.

Outside of direct cyber threats to OT environments, a cyber compromise of an organisation's IT environment may inadvertently impact that organisation's ability to safely operate its OT systems. Malware infections may spread from IT systems to connected OT systems (even if those OT systems were not the primary target), and availability impacts to converged IT/OT infrastructure management platforms may result in an inability to adequately monitor or manage OT systems.

In summary, the business and cyber threat landscape means that further attention and investment is required to uplift the cyber security capabilities and controls which enable us to detect, prevent and respond to the cyber threats faced by our mission-critical OT systems.

2.5. Impacts on customers

Cyber threats are malicious activity of unauthorised individuals or organisations that compromise the security of information and communication systems. The threats include attempts to disrupt operations or access data by exploiting weaknesses in digital assets such as infrastructure, applications and systems or devices.

Cyber attacks can lead to severe consequence for electricity networks such as AusNet. A successful attack could compromise control over the physical network and digital systems used to operate the business. In turn, this could cause widespread and prolonged disruption of electricity. As the transmission network service provider for Victoria, the consequences could be severe; potentially leading to prolonged outages for all Victorian electricity customers. The impact to residential customers and economic activity would be extensive. Critically, electricity is also an enabler of other essential services including telecommunications.

The key risks of a cyber attack for our customers include:

- Higher risks of unplanned outages including wide-scale and prolonged outage events.
- Higher risks of compromising the physical safety of customers and the community in operating the energy system and restoring power after faults.
- Higher risks that customer energy resources including solar installations could be compromised as a result of an attack on our network.
- Higher risks of an unplanned outage of critical digital systems that prevents us from communicating with our customers, or publishing critical market data.
- Higher risks that customers' personal data could be compromised, stolen or inappropriately accessed.

2.6. Regulatory and compliance obligations

Critical infrastructure is a key target of cyber attacks due to the potential for severe consequences. The Australian Cyber Security Centre (ACSC) found recently that about 25 per cent of reported cyber security incidents involved Australia's critical infrastructure, and that electricity sector constitutes 30% of the reported cyber security incidents in critical infrastructure for 2023-2024[5].

For this reason, legislation and regulation are moving rapidly to ensure that critical infrastructure is protected from malicious cyber activity.

[5] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

Table 1 identifies key regulatory obligations that are critical to AusNet's cyber security practices.

Table 1 - Regulatory obligations underpinning cyber security functions

Regulatory Obligation	Description of obligations
Security of Critical Infrastructure Act 2018 (SOCI Act)	The SOCI Act seeks to manage national security risks in Australia's critical infrastructure including energy. The obligations include: • a requirement to develop a register of Critical Infrastructure Assets • mandatory cyber incident reporting to the Australian Cyber Security Centre • information and directions powers
Privacy Act 1988 and Information Privacy Act 2014	The obligations require us to maintain strong controls and security on the accessibility of customer data as well as appropriate availability of data.
National Electricity Rules	Under section 4.11.2(c) of the NER, we must comply with AEMO's Standard for Power System Data Communications which operates in parallel to the SOCI Act identified above. Section 4 of the Act requires that cyber, physical and network security considerations are appropriately addressed by all parties including through robust programs and reporting frameworks to adequately and continuously manage security risks that could adversely impact power system communications and supporting systems and infrastructure.
Enhanced Response and Prevention Act 2024 (SOCI Amendment Act)	The Act sets out the obligation to manage the cyber risk to the critical infrastructure, including energy sector. The relevant obligations include: • extending critical assets obligation to the systems holding business critical data • responding to the government request to address serious deficiencies within their risk management programs, if any. • Taking direction from the government to manage all hazards incidents
Cyber Security Act 2024	Act seeks a mandatory requirement for reporting of ransomware ransom payments.

2.7. Industry framework - AESCSF

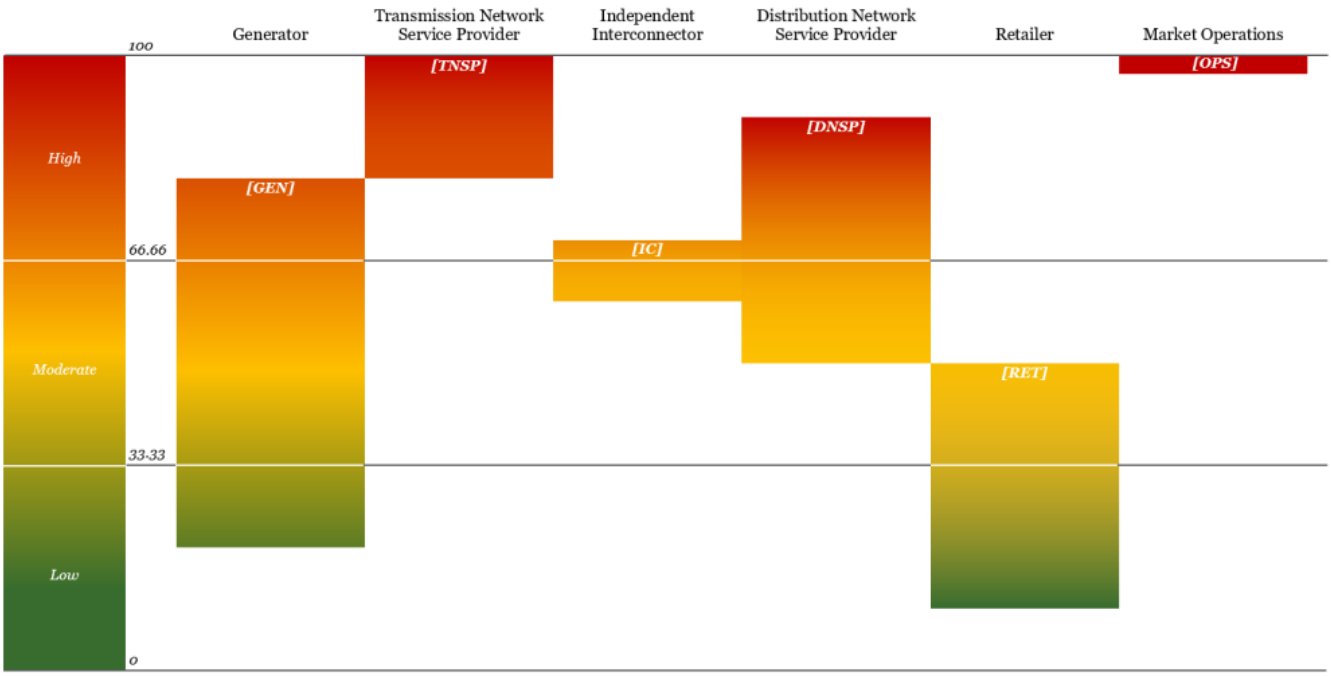
Consistent with our peers in the sector, AusNet aligns to the Australian Energy Sector Cyber Security Framework (AESCSF) to establish, uplift and measure the maturity of our cyber security capabilities. The AESCSF was developed in 2021 by the Australian Energy Market Operator (AEMO) in collaboration with industry and government stakeholders including the Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC), and the Cyber Security Industry Working Group (CSIWG) to raise the level of cyber maturity across the energy sector by helping market participants to assess, benchmark, and enhance their cyber security capabilities.

The AESCSF provides a consistent baseline on which market participants can develop risk management practices that align with regulatory obligations, including the SOCI Act. By providing a tailored approach to managing cyber risk, the AESCSF strengthens cyber maturity and resilience across the sector. In 2023, AEMO updated the AESCSF to Version 2 to align with current international standards, and to address emerging technologies and the evolving cyber threat landscape. AusNet has chosen to adopt this updated version.

The framework defines cyber security practices across a number of domains and objectives, grouped into three Security Profiles (SPs) defined by the Australian Cyber Security Centre (ACSC) in consultation with AEMO and industry representatives. This tiered risk-based approach ensures that participants target the appropriate maturity level based on their criticality within the energy sector.

The following diagram demonstrates the relative criticality of market participants based on their role(s) in the electricity sector.

Figure 1 - Criticality Bands by Market Role – AESCSF Electricity Criticality Assessment Tool (E-CAT) 2023 (p5)



While AESCSF Version 2 does not mandate that market participants achieve certain Security Profiles (SPs) based on their criticality, AEMO's guidance is that organisations should target higher levels of cyber maturity in accordance with their criticality. As a high-criticality market participant, given our joint role as a Transmission and Distribution Network Service Provider, AusNet believes it is prudent for us to work towards achieving SP-3 within the FY2027-31 regulatory period.

2.8. AusNet Enterprise Risk Management Framework

Consistent with best industry practice, AusNet is risk averse in our approach to preventing cyber security events. We adopt a 'so far as is reasonably practical' approach. This involves regularly assessing the macro-environment and receiving intelligence from Government on risk levels and vulnerabilities.

As a combined distribution and transmission provider, AusNet as an organisation must meet the highest requirement of all the market roles it plays (as per Figure 1 above). Our risk aversion reflects our role as Victoria's transmission network service provider, and the elevated degree of risk to our customers from a cyber security event. As detailed in Section 2.7, transmission network service providers are the highest risk criticality together with market operations. This reflects that a widescale outage of our transmission services could:

- result in a loss of supply of all Victorian electricity customers, placing at risk the lives of vulnerable customers in the state and causing significant impact to economic activity.
- have cascading impacts for other customers and participants in the integrated NEM.

While our enterprise risk level is largely based on our transmission electricity services, we note that the distribution network also has a high degree of risk identified under the AESCSF. This risk is also increasing due to integration of our network with our customer's energy resources such as solar panels that increase both the consequence of a cyber event and the potential for cyber attacks to intrude from CER.

Specific to the distribution network, we have assessed key risks using the Enterprise Risk Management Framework. This assessment is focused on 3 risk scenarios, as detailed below. Our risk assessment, and these scenarios, considers the threat landscape detailed in the prior sections.

Compromised operation of the network

Cyber attacks have the potential to directly impact our network operations, resulting in loss of supply to our customers. The key types of risks we considered were:

- Widescale outage – Cyber attack results in a widescale loss of supply to a large number or all of Victorian electricity customers.
- Loss of automated controls – Field workers are required to take direct control of the network to directly restore electricity, resulting in inconsistent ability to provide power and impacting AusNet's productivity whilst restoration efforts take place.
- Increase length of unplanned outage – Critical operational systems being compromised or rendered unavailable, potentially leading to increased length of unplanned network outages.
- Delays to planned maintenance – Critical operational systems being compromised or rendered unavailable, potentially leading to reduced staff productivity.

Compromised data

Cyber attacks can target information held in our systems. This risk relates to:

- Theft of personal and commercial information about customers, employees and contractors and inability to operate systems supporting the key business services such as payroll and financial transactions
- Delays in being able to publish key data to the market - Critical operational systems being compromised or rendered unavailable, potentially leading to an inability to publish key data to the market in a timely fashion

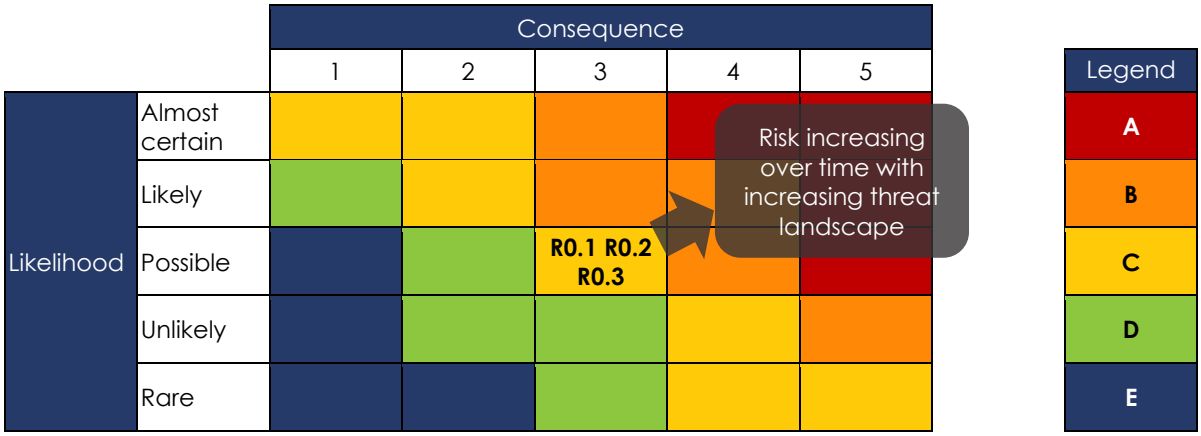
Compromised staff operations

Cyber attacks can also target corporate and asset systems leading to two types of risks:

- Lost staff productivity – Staff are unable to access technology systems operational capacity, impacting our employee productivity and our ability to interact with our customers
- Compliance risk – Staff are unable to access information or reporting systems, leading to non-compliant activity.

Figure 3 shows our assessment of the network risk with the current systems and platforms in place as of end-2024. Importantly, if all controls remain unchanged, over time the risk will increase as the threat landscape increases, for example new attack vectors and technologies such as AI. These risks are reassessed to determine the residual risk under each option. Risks of highest concern are rated red, whereas those of lowest concern are rated blue.

Figure 2 – Risk assessment of current state



	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R0.1	Compromised operation of the network	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R0.2	Compromised data	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R0.3	Compromised staff operations	Possible: May occur to our systems	3: Severe event impacting effectiveness of organisation	C

3. Recurrent investment

The purpose of this section is to identify the overarching drivers of recurrent capex investment in cyber security for the FY2027-31 regulatory period. This investment is focused on maintaining the cyber security systems and applications that were implemented through the FY2021-26 period, to maintain current capabilities.

3.1. Identified Needs

As detailed in Section 2, during the FY2021-26 period we have made significant investments to uplift our cyber security infrastructure, systems and practices across our network businesses. These investments have us on track to achieve Security Profile 2 (SP-2), as defined in version 1 of the AESCSF, in the current period.

We have identified that the systems that deliver these capabilities will require refresh during the FY2027-31 regulatory period. This investment relates to updating our security appliances, application firewalls, perimeter firewalls, and security information and event management tools. These refreshes will ensure that these systems and applications remain current with latest patches, configurations and vendor support, so as to fully maintain their current level of capability.

As detailed in Table 2 below, a total of $16.2 million capex is forecast as required to maintain the cyber security capability levels reached by the end of the 2021-26 regulatory period.

Table 2 - Proposed recurrent expenditure

Recurrent capex	Description of need
[CIC]	Infrastructure and Application Security and Vulnerability Patching.
[CIC]	Network Security refresh in IT. Includes: [CIC]
[CIC]	Network Security refresh in OT. Includes: [CIC]
[CIC]	Security Assets in IT that have on-premises components. Includes: [CIC]
[CIC]	Security Assets in OT that have on-premises components. Includes: [CIC]
[CIC]	Governance, Risk and Compliance (GRC) Platform Refresh

3.2. Options assessment

In developing this business case we have focused on the AER's expectations on the method and approach that should be applied to proposed recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019.

The AER identifies multiple approaches to assess recurrent expenditure. In terms of bottom-up analysis, the AER recognises that recurrent expenditure relates to maintaining an existing service and that it will not always be the case that the investment will have a positive NPV. It expects that a business case will consider possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency).

To give effect to this methodology we used risk-cost analysis to determine the optimal strategy for recurrent expenditure on cyber security spend categories as set out in Table 2. Option 1 was to actively manage without lifecycle refreshes. Option 2 was to refresh our metering systems in line with vendor recommendations.

Table 3 – Recurrent expenditure options

OPTION	SUMMARY
Option 1: Actively manage without vendor support	Operate our control, metering and business systems without performing updates, patching or refreshes and actively manage the risks in-house
Option 2: Perform lifecycle refreshes **(Recommended option)**	Where prudent and efficient, performing refreshes, upgrades and patching of cyber security systems in line with vendor recommendations and maintaining vendor support

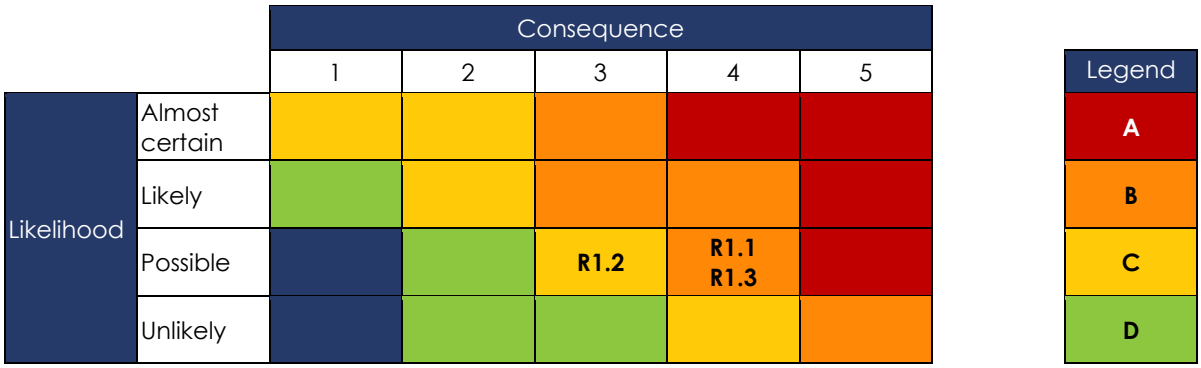
3.2.1. Option 1 – Actively manage without vendor support

Under this option, we would undertake minimal refreshes and seek to actively manage the risks of operating our cyber security systems and applications beyond their expected or recommended cycle. This would effectively operate the systems and applications longer than the recommended refresh period. We would seek to actively manage the risks of systems and applications that present security vulnerabilities or fail in service.

There are a number of risks associated with this option, as highlighted in the assessment below relative to our Enterprise Risk Management Framework. Figure 3 shows the risk level matrix to which we have assessed each of risks within the options. Risks of highest concern are rated red, whereas those of lowest concern are rated blue.

We consider that overall, this option has elevated risk, does not meet the needs of the business and is therefore not a recommended option. Without vendor support it is likely there will be more unpatched cyber security systems with vulnerabilities, which will see our cyber security environment degrade relative to current capabilities and risk levels. To some degree these can be partly mitigated with additional monitoring, however this would require additional support resources which would result in an opex uplift. If a cyber breach was to occur, it is more likely to spread through these unpatched vulnerabilities increasing the operational consequence of the breach as shown in Figure 3 (Compromised Network Operations risk R1.1). Additionally, the compromised staff operations as a result of the spread of the compromise would impact more staff operations and will take longer to restore (Compromised Staff Operations R1.3). As a result this option is considered unacceptable.

Figure 3 – Risk Analysis – Option 1 Recurrent Expenditure



	Rare						E

	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R1.1	Compromised operation of the network	Possible: May occur to our systems	4: Major impact to customers, regulatory impacts and litigation	B
R1.2	Compromised data	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R1.3	Compromised staff operations	Possible: May occur to our systems	4: Major impact to effectiveness of organisation	B

3.2.2. Option 2 – Perform lifecycle refreshes (recommended option)

This option involves refreshing cyber security systems and applications in line with vendor recommendations. This ensures that the systems receive required patching, security and functionality upgrades, and maintain vendor support.

This option is recommended as it maintains the associated risks to as low as practical and reducing likelihood and minimising consequences relative to Option 1. This can be seen in Table 4 where all risks are rated as C, maintaining the current risk profile set at end-2024. While required investment is $16.2 million, Option 2 is the recommended option based on this risk reduction.

Note that this option sees AusNet only maintain the forecast SP-2 maturity level, and does not consider the ever-increasing cyber threat landscape requiring new capabilities. Further non-recurrent investment will be required to ensuring this risk level is maintained over time, with capability uplift investments detailed in the following Section 4. Maintaining current base capabilities is a required base level from which these new capabilities can be built.

Figure 4 – Risk Analysis – Option 2 Recurrent

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain					
	Likely					
	Possible			**R2.1 R2.2 R2.3**		
	Unlikely					
	Rare					

Legend
A
B
C
D
E

	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R2.1	Compromised operation of the network	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R2.2	Compromised data	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R2.3	Compromised staff operations	Possible: May occur to our systems	3: Severe event impacting effectiveness of organisation	C

4. Non-recurrent investment

The purpose of this section is to identify the overarching drivers of non-recurrent capex in cyber security for the FY2027-31 regulatory period. This investment is focused on uplifting our cyber security capabilities in line with the increasing threat landscape and industry standards.

4.1. Drivers of investment

While we have significantly improved our cyber security practices in the current regulatory period, we see a need to continue to evolve our capabilities to keep pace with increased cyber threats and associated uplifts in industry standards. The key drivers of cyber security in the FY2027-31 period are identified below.

Increased cyber threat

The risk of a cyber attack has significantly increased over the last 5 years. This is due to increased reliance on digital technologies, which are also becoming more inter-connected. There is also a heightened level of cyber threats due to general evolution of cyber malicious activity, and a more disruptive socio-political global environment. There have been a spate of high-profile cyber attacks including:

- Optus – The telecommunications carrier was subject to a cyber attack that resulted in the details of 10,000 customers details being released publicly on the internet.
- Medibank – A cyber attack enabled personal data such as names, addresses, dates of birth, phone numbers, email addresses to be placed on the dark web.

Our intelligence suggests that critical infrastructure providers such as electricity networks continue to be a target of cyber attacks, as described in Section 2. The attack that struck the Ukraine electricity system in 2015 through a series of power outages is a stark reminder of the potential for cyber attacks to have the potential to impact loss of supply. In a more complex geo-political environment, there is increased risk of state sponsored sabotage that directly targets the physical operation of the network.

Change in industry standard on cyber capabilities

In the above context, it is vital that cyber security continues to keep pace with emerging threats. This has been reflected in version 2 of the AESCSF released by AEMO in 2023. The Framework was reviewed to align with current international standards and address emerging technologies and the evolving cyber threat landscape. The update resulted in a further 72 capabilities, creating a more mature framework for the energy industry. It has also meant that all Security Profile levels include additional capabilities.

Inter-relationship with customer energy resources

A key driver of improved cyber security is the increasingly complex inter-relationship between our physical network and the customer energy resources (CER) of our customers including solar and electric vehicles including technologies such as the solar back stop. This means that cyber security needs to consider intrusion entry points from CER, and must also consider the consequential impact to customer devices from attacks on our physical infrastructure.

4.2. Identified need

Underlying non-recurrent expenditure is an identified need to mature our cyber capabilities for electricity networks from an SP2 level under version 1 of the AESCSF to a SP3 level under version 2 of the AESCSF. This is due to the following reasons:

- Due to increased risk of cyber attacks, it is prudent as an electricity network operator to achieve the highest maturity rating under the AESCSF.
- This aligns with our cyber security risk framework which adopts the lowest risk tolerance for cyber security.
- Recent events and customer engagement demonstrates the value that customers place on cyber security, for the protection of their personal information

The key focus areas for AusNet to uplift to SP3 levels include:

- Cybersecurity Architecture: Planning, designing, and managing the cybersecurity control environment. Refer to Defensible Architecture/Zero Trust Architecture below.
- Risk Management: Incorporate leading risk management practices and enhance coordination between cyber and enterprise risk management.
- Third-Party Risk Management: Effectively address third-party IT and OT cybersecurity risks, such as sensitive data in the cloud and vendors with privileged access, as well as build supply chain security into organisational culture.

Table 4 sets out the specific identified needs to reach SP3 security level.

Table 4 – Identified gaps in capability to meet SP3 level

System or Application	Description of current function and identified need
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]

[CIC]	[CIC]
[CIC]	[CIC]

4.3. Options assessment

In developing this business case for the non-recurrent element of cyber security, we have focused on the AER's expectations on the method and approach that should be applied to proposed non-recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019. The AER expects that networks will evidence the need and demonstrate prudency and efficiency of the investment. it is expected that options of scope and timing (to demonstrate prudency) and options for alternative implementation approaches (to demonstrate efficiency) will be evaluated.

As per the AER guidelines, we have examined credible options for our cyber capability maturity, with assessment relative to residual risk and cost to implement. We identified and assessed two credible options for target state maturity levels (Security Profiles) by the end of the FY2027-31 regulatory period. These are shown in Table 5 below.

Table 5 – Non-recurrent expenditure options

OPTION	SUMMARY
Option 1 – Achieve AESCSF Version 2 Security Profile 2	We would invest to only achieve the updated capabilities for SP2 under version 2.0 of the AESCSF by the end of the FY2027-31 regulatory period
Option 2 – Achieve AESCSF Version 2 Security Profile 3	We would invest to achieve the updated capabilities for SP3 under version 2.0 of the AESCSF by the end of the FY2027-31 regulatory period.

Non-credible options

Our needs identification has largely been based on the cyber security requirements for our joint role as a transmission and distribution network service provider. It could be argued that the consequences of a cyber attack impacting our distribution network are lesser than transmission as there would be fewer impacted customers; however, as part of our analysis we considered whether it was technically or economically feasible to develop a standalone approach to uplifting cyber security for our distribution network separate from the transmission network. Our analysis found that:

- It would be highly impractical to develop standalone cyber capabilities for the distribution network given that our technology infrastructure, systems, applications and devices are largely shared across our transmission and distribution networks. This would lead to duplication of cyber capabilities and services, dramatically increasing complexity and cost.
- It would also be uneconomic to develop standalone cyber capabilities for the distribution network. In our planned approach, the distribution network has been allocated 25 per cent of the total cyber security investment under our Cost Allocation Methodology, representing significant efficiencies for distribution customers compared to those of peer organisations whose distribution networks have to bear the full costs of their cyber security programs.
- We also considered whether we should continue to align our cyber program to version 1 of the AESCSF, however we believe it would be imprudent for AusNet to not keep pace with AEMO's development of the AESCSF in light of the changing threat environment and the broader direction being taken by the sector.

4.3.1. Option 1 – Achieve AESCSF Version 2 Security Profile 2

Under this option, we would only address a subset of each of the shortfall areas in Table 4 of Section 4.2 focusing on those aspects related to the SP2 capabilities. The total cost would be $6.8M reflecting the distribution allocation required to bridge the gap from AESCSF Version 1 Security Profile 2 (V1 SP2) to AESCSF Version 2 Security Profile 2 (V2 SP2). This reduces the AESCSF practices from 354 required to reach SP3 V2 to 275 required to reach SP2 V2, which includes the 75 new practices identified as part of Version 2. As the AESCSF calls out practices, these are still expected to span all or part of the focus areas mentioned in Section 4.2.

AESCSF V1 SP2 was considered reasonable maturity target for a combined distribution and transmission network operator given the risk level at the time we developed our current period regulatory proposal in 2020. However, the risk of cyber attack in the current threat environment is far higher than 5 years ago and is likely to increase between now and the end of the next regulatory period. Our analysis considered the growing level of cyber security risk by not going beyond the SP2 level of maturity. Figure 5 sets out the analysis.

Figure 5 - Risk Analysis – Option 1 Non-recurrent (forecast at end of FY2027-31 regulatory period)

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain					
	Likely					
	Possible			**R3.2 R3.3**	**R3.1**	
	Unlikely					
	Rare					

Legend
A
B
C
D
E

	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R3.1	Compromised operation of the network	Possible: May occur to our systems	4: Major impact to customers, particularly if propagated to transmission network, with regulatory impacts	**B**
R3.2	Compromised data	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	**C**
R3.3	Compromised staff operations	Possible: May occur to our systems	3: Severe event impacting effectiveness of organisation	**C**

We consider that overall, this option has elevated risk, not tolerated per our enterprise risk management framework and is a non-viable option. This is primarily because a compromise of AusNet through the distribution focused cyber controls which under this option are targeting SP2 has the potential to propagate to the transmission network resulting in a higher network operations consequence (risk R3.1 above). Cyber attackers will focus on the weakest point when targeting an organisation.

Under this option, we would have only a limited program that does not address the identified needs in Section 3. As reflected in Figure 6, this option would see the following risks continue to be imposed on AusNet and our customers:

- Potential cyber-intrusion causing comprised operation of the network through via OT systems, or software that has a network control or automation function.
- Further risk areas for cyber intrusion including through devices, and through an inadequate threat detection and response system.
- Theft of customer or market data through unauthorised access of protected data.
- Inability to keep up with defence mechanism for emerging technology such as AI.

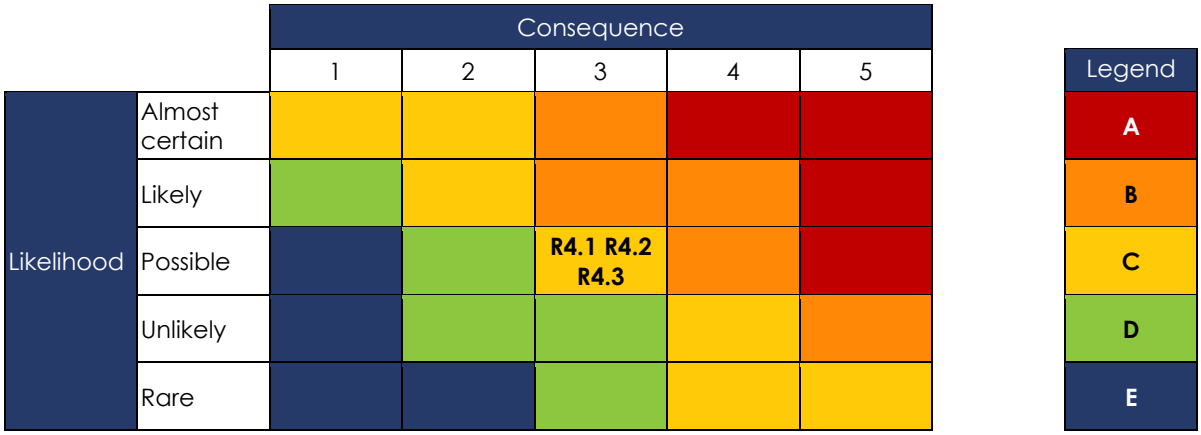
4.3.2. Option 2 – Achieve AESCSF Version 2 Security Profile 3

Under this option, AusNet would develop programs that would address all the gaps in our cyber security environment identified in 4 of Section 2. Appendix A sets out the detailed program scope and costs. The total cost would be $8.7M reflecting the distribution allocation required to bridge the gap from AESCSF Version 2 Security Profile 2 to AESCSF Version 2 Security Profile 3.

Figure 6 shows that the programs are focused on reducing the risks relative to option 1 and to achieve a risk level as low as reasonably practical at the end of the FY2027-31 regulatory period.

While the costs option 2 are higher than option 1, AusNet considers that the reduction in overall risks is significant and as result this option is recommended.

Figure 6 – Risk Analysis – Option 2 Non-recurrent (forecast at end of FY2027-31 regulatory period)



	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R4.1	Compromised operation of the network	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R4.2	Compromised data	Possible: May occur to our systems	3: Severe impact to customers and regulatory implications	C
R4.3	Compromised staff operations	Possible: May occur to our systems	3: Severe event impacting effectiveness of organisation	C

5. Recommended option

Based on our assessment in Sections 3 and 4 we found that achieving AEMO AESCSF Version 2 Security Profile 3 is the preferred option. Achieving this target state will require:

- Recurrent investment of $16.2 million to perform lifecycle refreshes on our current cyber security systems and applications, as detailed in Section 3 Option 2. This enables AusNet to maintain current risk profile against AESCSF Version 1 Security Profile 2 based on the current 2024 threat landscape. This option additionally provides the base layer required from which to implement additional cyber security capabilities.
- Non-recurrent investment of $8.7 million to uplift capabilities to achieve AESCSF Version 2 Security Profile 3, as detailed in Section 4 Option 2. This enables AusNet to minimise risk in the ever increasing cyber threat landscape out to 2031 at the organisational level.

These recommended options align with the AEMO AESCSF Version 2 obligations in line with AusNet's market roles in distribution and transmission. This option reflects AusNet's Cost Allocation Methodology for fair allocation, while efficiently meeting the overlapping obligations due to AusNet multiple market roles.

On this basis, the recommended options:

- Enable AusNet to remain compliant with our obligations under the NER and our Distribution licence requirements;
- Minimise cyber security risk across the organisation as far as reasonably practicable, and;
- Result in a consistent and optimised cyber security capability for the organisation across all market roles.

Appendix A – Non-recurrent capex

Table 6 sets out the programs of non-recurrent investment to address the identified gaps in capabilities required to meet Security Profile 3, as per AESCSF Version 2, practices by the end of the FY2027-31 regulatory period.

Table 6 – Non-recurrent Capex by Program

Program / Initiative	Description	Total cost	Distribution Allocation
[CIC]	[CIC]	[CIC]	[CIC]
[CIC]	[CIC]	[CIC]	[CIC]
[CIC]	[CIC]	[CIC]	[CIC]

[CIC]	[CIC]	[CIC]	[CIC]
[CIC]	[CIC]	[CIC]	[CIC]

[CIC]	[CIC]	[CIC]	[CIC]
[CIC]	[CIC]	[CIC]	[CIC]

[CIC] [CIC] [CIC] [CIC]

AusNet

Follow us on