AusNet

Transmission Revenue Reset

TRR (2027-32)

Revised Proposal Addendum:

Cyber Security

Date: 1 September 2026

Table of Contents

Document history

DATE	VERSION	COMMENT
30/07/2026	V1.0	Draft business case addendum
18/08/2026	V2.0	Updated draft incorporating SME feedback
30/08/2026	V3.0	Final addendum for submission

Related documents

DOCUMENT	VERSION	AUTHOR
4.2.09 AusNet - Revised Digital NPV model - 1 Sep 2026 - SOCI ACT PROTECTED	V2.0	AusNet Services

Approvals

POSITION	DATE
Digital & Technology – Strategy, Regulatory and Partner Management	August 2026
Digital & Technology – Cyber Security	August 2026
Digital & Technology – Architecture	August 2026
Transmission – Strategy and Regulation	August 2026

Executive Summary

Cyber security is fundamental to the safe and reliable operation of AusNet's electricity transmission network. As digital technologies become increasingly interconnected across our operational and corporate environments, cyber threats are becoming more sophisticated, persistent and consequential. As a provider of critical electricity infrastructure, AusNet considers it prudent and necessary to achieve Security Profile 3 (SP3) under Version 2 of the Australian Energy Sector Cyber Security Framework (AESCSF) in the coming regulatory period. This target maturity level was accepted in the Australian Energy Regulator's (AER) Draft Determination.

AusNet's initial proposal was developed following a comprehensive cyber resilience assessment and recommends an integrated program of recurrent and non-recurrent investments to uplift cyber security maturity from the forecast AESCSF V2 SP1 position at the end of the current regulatory period to AESCSF V2 SP3 by 2032. The program addresses identified gaps across Information Technology (IT) and Operational Technology (OT) environments and is designed to manage cyber risks as far as reasonably practicable for a high-criticality transmission network operator.

AER Draft Determination

The AER's Draft Determination accepted the need for AusNet to achieve AESCSF V2 SP3 and accepted most of the proposed expenditure. However, it identified several areas where further justification was sought, including perceived overlap between programs, alternative sequencing of activities, and whether certain programs were necessary to achieve AESCSF V2 SP3. The AER's Draft Determination included a $8.4 million (15%) capex reduction to the cyber security program.

AusNet's Revised Proposal response

This addendum responds directly to the AER's feedback. Recognising the AER's feedback, AusNet has completed a detailed assessment of cyber risks, controls, control effectiveness and AESCSF requirements. This assessment revalidated the original program and confirmed that all nine investment programs remain necessary to address identified control gaps and achieve AESCSF V2 SP3 maturity. The assessment also strengthened the linkage between cyber risks, required controls and proposed investment activities, providing additional evidence that the proposed program is prudent, efficient and targeted.

The additional analysis demonstrates that the programs identified by the AER as potentially overlapping actually deliver distinct functions, address different AESCSF practices and provide different cyber security capabilities. Programs relating to identity management, security architecture, threat detection, OT security, governance and risk management are complementary and interdependent, but they are not duplicative. Collectively they are required to address the full range of AESCSF V2 SP3 obligations and control effectiveness gaps across the organisation.

The addendum also demonstrates that the proposed sequencing within data protection and IT/IoT security uplift reflects dependencies between the phases of each program. Re-phasing would require later-stage controls to be implemented before the required inventories, classifications, baselines and controlled-access mechanisms are established. Deferring or re-phasing these programs, as proposed in the Draft Determination would disrupt critical dependencies, delay downstream delivery, increase implementation cost and risk, and materially reduce AusNet's ability to achieve AESCSF V2 SP3 in the forthcoming period. The proposed timing is therefore not discretionary; it reflects the minimum practical sequencing required to deliver the program efficiently, meet emerging regulatory obligations and strengthen the cyber resilience of AusNet's critical electricity infrastructure.

The additional analysis also confirms that the programs removed or reduced in the Draft Determination are not discretionary enhancements; they are necessary components of the integrated capability required to achieve and sustain AESCSF V2 SP3 maturity. This includes capabilities related to secure software development, security architecture, governance, assurance, risk management and information protection. These capabilities are interdependent and support the effectiveness of the broader cyber program; removing or materially reducing any of them would create substantive control gaps and prevent full implementation of the applicable AESCSF V2 SP3 practices.

Revised Proposed expenditure

Accordingly, AusNet maintain that our original cyber security proposal is prudent and efficient, and is required in full as the minimum practical, proportionate and sustainable investment required to achieve and maintain the targeted AESCSF V2 SP3 maturity outcome. However, we accept the reduction (capex to opex recategorization) to cloud security and will fund that through our opex allowance. Our revised proposal capex forecast is provided in Table 1 below.

Table 1 Proposed capex expenditure required for Cyber Security program ($real 2025, Transmission network allocation)

ID	Program name	Total
Non-recurrent expenditure to reach AESCSF V2 SP3 maturity *(made up of below)*		**$34.5m**
ID01	Threat Detection and Response	$7.7m
ID02	Operational Technology (OT) Threat and Vulnerability Management	$7.7m
ID03	Identity Access and Management	$6.2m
ID04	Cloud Security	$0.3m
ID05	Data protection	$3.5m
ID06	Secure Software Development Lifecycle	$2.1m
ID07	Defensible / Zero Trust Architecture	$2.9m
ID08	OT/IoT Security Uplift	$3.5m
ID09	Cyber Governance and Risk Management	$0.4m
Recurrent expenditure to maintain existing cyber security capabilities (accepted in Draft Determination)		**$20.4m**
Total Cyber Security Capex		**$54.9m**

The additional information contained in this addendum addresses the matters raised in the AER's Draft Determination, clarifies the role and necessity of each investment program, and demonstrates that the original program scope and sequencing are required for AusNet to achieve AESCSF V2 SP3 in the upcoming period and maintain an appropriate level of cyber resilience for critical electricity infrastructure. The proposal represents the transmission network allocated costs of AusNet's whole of enterprise cyber security program, as detailed in Information Request #015 (AusNet - IR#015 (#72 EDPR) - Master Cost Build Up & Reconciliation - 20250204- CONF).

1. AusNet's Proposal and AER Draft Determination

The cyber threat landscape is increasingly challenging and complex due to greater digital interconnectivity and the rise of sophisticated attacks, as demonstrated by recent high-profile incidents[1]. As a critical infrastructure provider, AusNet must continually enhance our cyber security measures to safeguard our operations and customers. While our investments to date provide a foundation, ongoing investment to enhance capabilities is essential to address evolving threats, keep pace with updated industry standards, and respond to the Australian Government's strengthened cyber security strategy.

This section outlines our proposed cyber security investments and summarises the Australian Energy Regulator's (AER's) Draft Determination, which accepted the key components of AusNet's proposal.

1.1. Initial Submission Summary

AusNet relies on an increasingly interconnected suite of Operational Technology (OT), Information Technology (IT), applications and digital infrastructure to deliver safe and reliable electricity transmission services across Victoria. As detailed in our initial proposal business case, Cyber security threats are continuing to increase and new information released in June 2026 further supports this increasing risk[2]. As a high-criticality transmission network operator, it is essential to maintain strong cyber security posture to prevent significant impacts and disruptions to essential services for Victorian customers and the National Electricity Market.

The Australian Energy Sector Cyber Security Framework Version 2 was released in 2023 and raised industry expectations in relation to IT and OT systems security practices. As example, the AESCSF Version 2 requires 354 practices to achieve Security Profile 3, which is 72 more (an increase of 25%) than under AESCSF Version 1.

AusNet's most recent maturity assessment was undertaken in March 2025 and it found that due to the significant changes to the framework. AusNet was assessed at [C-I-C] . Our immediate objective is to achieve AESCSF V2 SP1 by the end of the current regulatory period, March 2027.

As a provider of electricity transmission services, AusNet is classified as critical infrastructure and considers that AESCSF V2 SP3 is the most prudent level of cyber security maturity. Our options assessment evaluated the risk-benefit of varying maturity target states and confirmed SP3 as the recommended target. As the operator of three networks using many shared and interconnected digital systems and infrastructure, our cyber security program encompasses the whole of AusNet with costs allocated to each network in accordance with our Cost Allocation Methodology (CAM).

From our target to achieve AESCSF V2 SP1 maturity at the end of the current regulatory period, AusNet needs to implement additional controls to comply with AESCSF V2 practices to reach SP3 maturity. Our proposed expenditure encompassed these requirements, along with recurrent expenditure to maintain existing cyber security capabilities. AusNet's proposal represented:

- Non-recurrent capex of $34.7 million, together with $18.0 million of new recurrent opex, to uplift AusNet to AESCSF Version 2 Security Profile 3 and maintain the target
- Recurrent capex of $20.4 million required to refresh existing systems and avoid degradation of current controls.

The recommended option represents total expenditure of $73.1 million (real FY2025, transmission network allocated costs), over the TRR 2027-32 period. This option was recommended as it aligns with AESCSF V2 SP3 requirements and meets AEMO's expectations for cyber security for high-criticality infrastructure. Achieving AESCSF V2 SP3 compliance will also reduce AusNet's material IT and OT cyber risks while establishing a sustainable cyber security capability to address the evolving threat landscape. It is the only option that reduces AusNet's material IT and OT cyber risks below our enterprise material risk threshold, supports ongoing regulatory compliance, and establishes a sustainable cyber security capability across AusNet's IT and OT environments.

[1] For example, the December 2025 cyber attack on Poland's energy sector including 30 wind and solar plants and a combined heat and power plant. The intent of the attack was purely destructive and used new and complex attack vectors and methods.
[2] https://www.defenceconnect.com.au/land/18445-active-cyber-threats-to-australias-critical-infrastructure-warns-asio-boss

1.2. AER Information requests

Through the AER review process, AusNet provided further supporting information and clarifications regarding the proposed cyber security program in response to information requests. **Table 2** below outlines the key items addressed through these information requests.

Table 2: Summary of AER information requests related to Cyber Security

Ref	Summary of AER Question	Summary of AusNet's response
EDPR Cyber Addendum	The AER queried whether sufficient evidence existed to justify the proposed cyber security expenditure and demonstrate the underlying control effectiveness gaps.	As part of our EDPR Revised Proposal submitted on 1 December 2025, AusNet provided a detailed assessment of required cyber security controls and their current effectiveness. This assessment identified specific control effectiveness gaps which underpins the proposed cyber security program, with each initiative directly linked to improving control effectiveness and supporting progression towards AESCSF Version 2 Security Profile 3 maturity.
Cost Benefit Analysis	To support AusNet's proposed cyber security investment program, AusNet has undertaken a detailed cost-benefit assessment across our three regulated networks (transmission, distribution and gas). This was provided to the AER on 19 December 2025 after the submission of our Initial TRR Proposal.	The Cost Benefit Analysis provided our assessment of three options: maintain current cyber security maturity; achieve AESCSF V2 SP2; and, achieve AESCSF V2 SP3. It also demonstrated the cost allocation between the different business networks. The analysis demonstrated achieving AESCSF V2 SP3 to provides the greatest cost benefit.
IR006	The AER sought clarification of AusNet's proposed cyber security expenditure and how it related to current and new cyber security requirements.	Consistent with enhanced industry standards, AusNet advised that it shifted from AESCSF Version 1 to Version 2 which introduced 72 new practices. AusNet aims to achieve AESCSF V2 SP1 by the end of the current regulatory period. Our proposed program will improve cyber security maturity from this baseline during the next regulatory period to achieve AESCSF V2 SP3.
IR015	Q1. The AER requested a consolidated explanation of AusNet's cyber security compliance journey across the current and proposed regulatory periods.	AusNet advised that it progressed from below AESCSF Version 1 SP1 compliance at the start of the current period to achieving SP1 in 2023 and SP2 in 2024. Following the release of AESCSF Version 2, the program was refocused to achieve AESCSF Version 2 SP1 by the end of the current period.
IR015	Q2. The AER requested detailed justification of cyber security program costs, including the cost build-up of the initiatives introduced in this business case and cost differences between TRR business case and the earlier EDPR business case.	Provided a detailed breakdown of the proposed cyber security costs and explained the key differences between the TRR and earlier EDPR business cases.
IR015	Q3. The AER requested a consolidated view of initiative costs and benefits, Transmission and Distribution allocations, preferred investment options and expenditure timing across the relevant regulatory periods.	AusNet provided a consolidated reconciliation model containing initiative costs, allocations and expenditure timing. AusNet confirmed that AESCSF Version 2 SP3 is the preferred option for both Transmission and Distribution, costs are allocated according to the CAM and that the model reconciles expenditure across the relevant regulatory proposals and periods.

Ref	Summary of AER Question	Summary of AusNet's response
IR015	Q4. The AER requested additional evidence supporting the cyber security cost-benefit assessment and confirmation of whether the cyber security risk mapping applies equally to the Transmission and Distribution businesses.	AusNet stated that its modelling is supported by Australian government threat assessments and real-life examples. A CBA model was provided. AusNet also confirmed that the cyber security risk mapping applies to both Transmission and Distribution because they share common infrastructure, systems and cyber-attack pathways.

1.3. AER Draft Determination feedback

The AER's Draft Determination accepted AusNet's target state maturity of AESCSF Version 2 Security Profile 3 as prudent based on demonstration of the cyber security risks and cost-benefit. The Draft Determination accepted the majority of proposed expenditure to reach this target state.

The AER's Draft Determination included all recurrent cyber security expenditure ($20.4 million), however adjustments were made to seven of the nine non-recurrent programs. The total impact of the AER' Draft Determination was to reduce non-recurrent expenditure by $8.4 million from $34.7 million to $26.3 million.

Table 3 below lists each of AusNet's proposed cyber security investment programs, the AER's Draft Determination and stated rationale for adjustments. The adjustments applied to AusNet's TRR program were similarly applied in AusNet's EDPR Final Determination received in March 2026.

Table 3: AER Draft Determination adjustments to cyber security investment programs (transmission network allocation)

Ref	Investment Program	AER Draft Determination	Proposal ($m Real 2025)	AER Reduction	Draft Determination ($m Real 2025)
ID01	Threat Detection and Response	The AER stated that there was overlap between ID01 and ID02. They consider that many solutions could address both objectives. The AER identified that shared solutions do work for other NSPs.	$7.7m	-26%	$5.7m
ID02	Operational Technology (OT) Threat and Vulnerability Management	No adjustment – fully accepted	$7.7m	0%	$7.7m
ID03	Identity Access and Management	No adjustment - fully accepted	$6.2m	0%	$6.2m
ID04	Cloud Security	Partial recategorization to opex	$0.4m	-33%	$0.3m
ID05	Data Protection	The AER disagreed with the proposed phasing of the initiatives within this program. The AER's alternative phasing resulted in a cost reduction.	$3.5m	-9%	$3.2m
ID06	Secure Software Development Lifecycle	The AER fully removed this program as their view is it is not mandated and not required to meet AESCSF V2 SP3. They stated that since it is not mandated, it must be supported by a cost benefit analysis.	$2.1m	-100%	$0
ID07	Defensible / Zero Trust Architecture	The AER considered that this program was a duplication of ID03 so was fully removed. The AER stated that ID7 requires significant re-architecting, not just a bolt-on solution, whereas ID03 looked more reasonable,	$2.9m	-100%	$0

		which was the driver for their decision to keep ID03 and remove ID7			
ID08	OT/IOT Security Uplift	The AER proposed an alternative phasing of the program, similar to ID05, although the exact reason for this was not stated.	$3.5m	-18%	$2.9m
ID09	Cyber Governance and Risk Management	The AER considered that this was a duplication of ID01 and ID02. The AER considered that our position in the AESCSF compliance summary was that appropriate governance mechanisms are already in place, so they did not feel that further governance was required.	$0.4m	-50%	$0.2m
		TOTAL NON-RECURRENT PROGRAMS	**$34.7m**	**-24%**	**$26.3m**
	Recurrent expenditure to maintain existing capabilities	No adjustment – fully accepted	$20.4m	0%	$20.4m
		TOTAL CYBER SECURITY PROGRAM	**$55.1m**	**-15%**	**$46.7m**

Note: rounding may affect calculation of percentage reductions

2. AusNet's Revised Proposal Addressing AER Feedback

AusNet has developed a suite of programs that will deliver increased cyber security maturity from an initial position of AESCSF V2 SP1 at March 2027 to AESCSF V2 SP3 in the coming regulatory period. The investment programs have been developed to address gaps and deficiencies in our systems and practices based on detailed internal and external assessment against the requirements of AESCSF Version 2.

We maintain our view that all the programs proposed in our initial submission are required; that each delivers specific elements of the AESCSF, and that AESCSF V2 SP3 can only be achieved by fully implementing the programs. The AER Draft Determination has proposed material reductions to the proposed investment that we believe would prevent us from achieving the target cyber security maturity required for AusNet.

We acknowledge the AER's draft determination for program ID02 (Operational Technology OT Threat and Vulnerability Management), ID03 (Identity Access and Management) and ID04 (Cloud Security). For Cloud Security, we accept that $138k capex was reallocated to opex and we will absorb the opex within the allowance provided in the draft determination.

However, we maintain that the expenditure for all other programs is prudent and necessary to achieve AESCSF V2 SP3. To address the AER's feedback, our revised proposal includes further information and clarity regarding the scope of each program and its requirement to reach AESCSF V2 SP3. The following sections address the AER's concerns to show:

- there is no overlap between the programs,
- the sequence of deploying the programs is optimal, and
- all the programs are required to meet the requirements of the AESCSF V2 SP3.

2.1. Overview of how all our programs are required to achieve AESCSF V2 SP3

Our non-recurrent cyber security maturity enhancement proposal comprises nine programs that are each focused on addressing specific elements of the AESCSF V2. The nine programs address different gaps that have been identified in our current systems and practices. Their scopes are distinct and complementary. While some programs contribute to common AESCSF maturity outcomes, each program addresses different control components, environments or assurance requirements.

The nine programs are summarised in **Table 4**, along with the number of AESCSF Version 2 practices that they each address to achieve SP2 and SP3.

Table 4 – AESCSF V2 practices addressed by each program

Program	Description	Total # SP2 practices	Total # SP3 practices
ID01 - Threat Detection and Response	Develops, operates and continuously improves AusNet's enterprise cyber defence capability and Security Operations Centre (SOC) operations, including threat detection, security monitoring, threat intelligence, threat hunting, detection engineering, incident coordination and response.	9	11
ID02 - OT Threat and Vulnerability Management	Establishes and operates OT-specific security which includes asset discovery, security monitoring, telemetry collection, threat detection, vulnerability identification and operational risk context for OT, Industrial Control Systems (ICS) and field environment that cannot be provided through conventional enterprise security tooling. ID02 builds the specialised OT capability that provides OT telemetry and intelligence to ID01, which performs enterprise correlation, investigation and response.	16	8
ID03 - Identity Access and Management	Establishes and governs identity, authentication, segregation of duties, least privileged access, account management for human and non-human accounts throughout its lifecycle with an assurance that access Is controlled, monitored and defensible.	6	2

Program	Description	Total # SP2 practices	Total # SP3 practices
ID04 - Cloud Security	Implements, operationalises and governs cloud security controls across the enterprise, ensuring all workloads are secured, continuously assessed and monitor against defined posture and protection standards.	8	2
ID05 - Data protection	ID05 implements the information protection requirements and design patterns established through ID07 and provides evidence of control operation and effectiveness to ID09. Defines and applies information classification, controls that detect or restrict inappropriate movement of information, encryption and privacy requirements throughout the information lifecycle. It implements the information-protection designs defined by ID07 and supplies control evidence to ID09.	14	4
ID06 - Secure Software Development Lifecycle	Embeds secure design, secure coding, security testing and release controls into software delivery for business applications, information technology, operational technology and industrial control systems. It uses architecture patterns from ID07 and supplies control evidence to ID09.It uses architecture patterns from ID7 and supplies control assurance and evidence to ID09.	2	5
ID07 - Defensible / Zero Trust Architecture	Defines AusNet's security architecture, trust boundaries, secure-access patterns and segmentation requirements, and implements priority Zero Trust access, device-trust, BYOD and enterprise segmentation controls.	12	5
ID08 - OT/IOT Security Uplift:	Implements preventive, engineering, access, hardening, segmentation and resilience controls within OT and IoT environments. Uses architecture and zoning requirements established through ID07 and prioritised weaknesses identified through ID02.	9	4
ID09 - Cyber Governance and Risk Management	Enhances AusNet's cyber governance framework by setting cyber security policy, managing cyber risk, overseeing regulatory compliance, independently assessing control effectiveness and tracking identified issues through to closure. ID09 evaluates evidence provided by control owners to determine whether controls are appropriately implemented and operating effectively. It provides governance and independent assurance but does not design security solutions (ID7) or implement and operate technical controls and services (ID01–ID08).	13	10

Note: Practice counts represent the number of non-compliant and partially compliant AESCSF V2 practices to which each program contributes. Multiple programs may contribute to achievement of the same AESCSF practice. Consequently, these counts are not additive and exceed the total number of unique practices requiring uplift.

The Australian Signals Directorate Critical Infrastructure Uplift Program (CI-UP)

In December 2025, following submission of AusNet's Initial TRR Proposal to the AER on 31 October 2025, the Australian Signals Directorate (ASD) conducted a review of AusNet's cyber security posture as part of its targeted Critical Infrastructure Uplift (CI-UP) program. The CI-UP program was offered to critical infrastructure operators across Australia to help address cyber security weaknesses that are actively targeted by sophisticated threat actors. Unlike a traditional compliance or best-practice assessment, the review is threat-informed and leverages ASD intelligence on adversary tactics, techniques and vulnerabilities being exploited against critical infrastructure operators. The review identified

[C-I-C]

and along with reinforcing the need for AusNet's proposed cyber security program also informed the identification of additional cyber security initiatives in to align with the new SOCI CIRMP Amended Rules (e.g., CI Fortify, subject of separate business case).

AusNet assessed each finding against the proposed cyber security investment program and confirmed that all nine programs contribute to the remediation of one or more identified gaps. Importantly, the findings associated with secure software development lifecycle, architecture governance, OT security, threat detection and control assurance directly align with programs that were reduced or removed in the Draft Determination. Removal of those programs would leave a number of ASD-identified gaps unresolved and increase the risk of not achieving AESCSF V2 SP3 maturity.

2.2. Requirement for Secure Software Development Lifecycle (ID06) to meet AESCSF SP3

The AER's Draft Determination removed ID06 on the basis that a Secure Software Development Lifecycle (SSDLC) is not specifically mandated by AESCSF V2 and is therefore not required to achieve SP3.

AESCSF V2 does not prescribe a particular software development framework, implementation methodology or technology product. It does, however, establish explicit SP3 security outcomes relating to secure software development, secure software procurement, application security review, software and firmware authenticity, security testing.

Table 5 identifies the relevant AESCSF V2 SP3 practices that will be addressed through the capabilities delivered by ID06.

Table 5: AESCSF V2 requirements relevant to secure software development

AESCSF V2 Practice ID	Security Profile	Practice detail
ARCHITECTURE-4b	SP-2	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices
ARCHITECTURE-4c	SP-2	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house
ARCHITECTURE-4d	SP-3	All software developed in-house is developed using secure software development practices
ARCHITECTURE-4e	SP-3	The selection of all procured software includes consideration of the vendor's secure software development practices
ARCHITECTURE-4f	SP-3	The architecture review process evaluates the security of new and revised applications prior to deployment
ARCHITECTURE-4g	SP-3	The authenticity of all software and firmware is validated prior to deployment
ARCHITECTURE-4h	SP-3	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events

Current capability gaps

[C-I-C]

How Secure Software Development Lifecycle (ID06) addresses the gaps

The proposed Secure Software Development Lifecycle program (ID06) establishes and operationalises required capabilities across software acquisition, design, development, testing, deployment and maintenance.

The program embeds security requirements into software delivery through secure development standards, automated security testing, software composition analysis, secrets scanning, secure code review, software integrity validation, secure procurement requirements and security gates.

The purpose of ID06 is therefore not to implement a particular software development framework. Industry frameworks such as OWASP SAMM v2 may provide implementation guidance, but the investment is directed at establishing the underlying people, processes, tooling and control evidence required to achieve and demonstrate the relevant AESCSF V2 maturity outcomes.

Importantly, ID06 is not proposed simply because these practices exist in AESCSF V2. AusNet's assessment has identified specific weaknesses in the current implementation and effectiveness of the corresponding controls. ID06 is the targeted capability uplift required to address those identified weaknesses.

Distinction from Defensible / Zero Trust Architecture and Cyber Governance and Risk Management programs

The proposed Secure Software Development Lifecycle program (ID06) performs a distinct role within AusNet's broader cyber security program.

- **ID06 – Secure Software Development Lifecycle:** establishes and operates software security controls throughout the software delivery lifecycle, including secure development, security testing, software integrity and secure procurement controls.
- **ID07 – Defensible / Zero Trust Architecture**: defines the enterprise security architecture, security standards, trust boundaries and reusable design patterns that solutions are required to follow.
- **ID09 – Cyber Governance and Risk Management:** provides governance and independent assurance by assessing whether controls are appropriately designed, implemented and operating effectively.

ID07 therefore defines the architectural requirements within which software solutions are designed, while ID06 implements and operates the software security controls required to meet those requirements. ID09 independently assesses the effectiveness of those controls. These capabilities are complementary but are not duplicative.

Secure Software Development Lifecycle (ID06) delivery initiatives

Table 6 below details and demonstrates how the identified capability gaps are addressed through the Secure Software Development Lifecycle program initiatives and links the remediation activities to the applicable AESCSF V2 requirements.

Table 6 – [C-I-C]

[C-I-C]

As part of our Revised Proposal development, AusNet considered whether the required outcomes could be achieved through existing project delivery, procurement, architecture and testing processes without the proposed ID06 investment. The assessment found that while elements of these activities exist today, they are applied inconsistently, are not sufficiently integrated into software delivery pipelines and do not provide the repeatability, automation, coverage or control evidence required to demonstrate SP3 maturity across Business, IT, OT and ICS environments.

Relying on existing processes would therefore leave identified control gaps unresolved and would not provide a sustainable organisation-wide software security capability. The proposed Secure Software Development Lifecycle represents the minimum practical and sustainable capability uplift required to address AusNet's identified software security control gaps and achieve required AESCSF V2 SP3 outcomes.

The program does not duplicate the architecture capability delivered through ID07 or the independent governance and assurance capability delivered through ID09. It provides the implementation and operational capability necessary to embed software security controls throughout the software lifecycle.

Without the proposed Secure Software Development Lifecycle program, AusNet would retain material gaps in secure software development, software integrity, secure procurement and application security testing, preventing the relevant AESCSF V2 SP3 practices from being consistently implemented and evidenced.

2.3. Both Zero Trust Architecture (ID07) and Identity Access and Management (ID03) are required by AESCSF V2 SP3

The AER's Draft Determination considered Defensible / Zero Trust Architecture (ID07) to duplicate Identity Access and Management (ID03) and removed ID07 in full. The AER also noted that ID07 appeared to involve significant re-architecting, whereas ID03 represented a more targeted security uplift.

In AusNet program design, Identity Access Management (ID03) and Defensible / Zero Trust Architecture (ID07) address different cyber security risks and operate at different layers of the security control environment. ID03 establishes and governs who or what is permitted access and at what level. ID07 establishes and implements the architectural controls that determine how, from where and through which trusted pathways that access can be exercised, and how connectivity is constrained across the environment.

The two programs are therefore complementary but are not substitutes for one another.

Distinct control objectives

ID03 focuses on identity governance, authentication, authorisation and access lifecycle management for human and non-human identities. Its' capabilities include strong authentication, privileged access management, non-human identity management, automated joiner/mover/leaver processes and periodic access certification.

ID07 focuses on reducing implicit trust and constraining how authorised access is exercised across AusNet environments. It establishes secure access pathways, device-trust requirements, enterprise security architecture standards, trust boundaries, security zoning and network segmentation controls designed to restrict unnecessary connectivity and lateral movement following compromise.

These distinctions are detailed in **Table 7** below.

Table 7: Distinction Between ID03 and ID07

Area	ID03 – Identity Access Management	ID7 – Defensible / Zero Trust Architecture
Primary objective	Ensure only authorised users and systems receive least-privileged access.	Ensure access is delivered through secure pathways and constrained by architectural controls.
Core question addressed	Who should be granted access and at what level?	Once access is granted, which are the secure access pathways
Primary focus	Authentication, authorisation and access governance.	Trust boundaries, connectivity, security zoning and secure access architecture.
Key capabilities	Strong MFA, Enhanced PAM/PIM, non-human account management, lifecycle automation and access certification.	Zero Trust access controls, BYOD restrictions, security architecture standards, network segmentation and security zoning.
Risk addressed	Unauthorised access and excessive privileges.	Excessive trust, unrestricted connectivity and lateral movement following compromise.
Example outcome	A vendor receives only approved access and uses MFA.	The vendor can only connect through approved access pathways and cannot move beyond authorised environments, including only being able to access from trusted sources
Implementation activities	Deploy identity and access management controls.	Implement BYOD controls, secure access pathways, security zoning and migration of systems into approved security zones.
What it does not do	Define trust boundaries, segmentation requirements or architecture standards.	Manage identities, provision access, certify access or operate privileged access controls.

Importantly, the distinction between the initiatives is not merely conceptual. It is reflected directly in the AESCSF V2 practices addressed by each initiative as detailed in **Table 8**.

Table 8: AESCSF V2 Practices Addressed by ID03 and ID07

Initiative	AESCSF Practices Addressed
ID03 – Identity Access and Management	ACCESS-1I, ACCESS-1J, ACCESS-2H, ARCHITECTURE-3C, ARCHITECTURE-3D, ARCHITECTURE-4G, ARCHITECTURE-5D, ARCHITECTURE-5E
ID07 – Defensible / Zero Trust Architecture	ARCHITECTURE-1B, ARCHITECTURE-1C, ARCHITECTURE-1D, ARCHITECTURE-1E, ARCHITECTURE-1F, ARCHITECTURE-1G, ARCHITECTURE-1H, ARCHITECTURE-1I, ARCHITECTURE-1J, ARCHITECTURE-1K, ARCHITECTURE-2D, ARCHITECTURE-2E, ARCHITECTURE-2H, ARCHITECTURE-2I, ARCHITECTURE-2K, ARCHITECTURE-2L, ASSET-3C

Identity Access and Management (ID03) predominantly addresses identity, authentication and access-governance requirements. Defensible / Zero Trust Architecture (ID07) addresses the architecture, secure-access, trust-boundary and segmentation controls required to constrain how access is exercised across the technology environment.

Accordingly, removal of ID07 would leave security architecture and network-control gaps that cannot be addressed through identity controls alone.

ID07 is a targeted security implementation uplift

ID07 is not proposed as a wholesale re-architecture of AusNet's networks, applications or enterprise systems. The investment establishes the required security architecture and implements priority controls needed to progressively achieve that architecture.

The program comprises three initiatives:

[C-I-C]

The detailed scope and boundaries of each ID03 and ID07 initiative are summarised in **Table 9** below.

Table 9: [C-I-C]

[C-I-C]

A vendor-access scenario illustrates why both capabilities are required:

[C-I-C]

Accordingly, ID03 establishes and governs access entitlement, while ID07 constrains how that entitlement can be exercised across the technology environment.

Alternatives considered

AusNet considered whether the required security architecture and Zero Trust outcomes could be delivered through existing architecture functions or by expanding ID03.

Existing architecture functions provide project-level design and review capability but do not establish and implement the enterprise-wide trust boundaries, reusable security patterns, security zoning standards, secure-access pathways, device-trust controls and priority segmentation improvements required to achieve the target maturity.

Expanding ID03 would also not provide an efficient substitute. Identity controls determine whether a user or system is authenticated and authorised; they do not establish network trust boundaries, determine permissible connectivity between environments, assess device trust or implement segmentation controls.

Attempting to deliver these capabilities through ID03 would therefore extend that program beyond its identity-management purpose while leaving the underlying architecture and network-control capability inadequately addressed.

Conclusion

Identity Access and Management (ID03) and Defensible / Zero Trust Architecture (ID07) address distinct control objectives and cyber security risks.

ID03 determines and governs who or what is permitted access and at what level. ID07 establishes and implements the architectural controls that determine how, from where and through which trusted pathways that access can be exercised, while restricting unnecessary connectivity and lateral movement across AusNet environments.

ID07 should therefore be viewed as a targeted security architecture and implementation uplift, rather than a wholesale re-architecture program. Its scope is complementary to, but not duplicated by, ID03.

[C-I-C]

2.4. Absence of overlap across Threat Detection and Response (ID01), OT Threat and Vulnerability Management (ID02) and Cyber Governance and Risk Management (ID09)

In the Draft Determination, the AER highlighted concern of potential overlap between program ID01 (Threat Detection and Response), ID02 (OT Threat and Vulnerability Management) and ID09 (Cyber Governance and Risk Management). On that basis the AER accepted ID02 in full, reduced ID01 by 26% and reduced ID09 by 50%, on the view that some capabilities appeared duplicated and that governance arrangements were already in place.

AusNet's position is that ID01, ID02 and ID09 deliver distinct, complementary and non-substitutable capabilities that operate at different layers of AusNet's cyber security operating model, and that each is required to achieve AESCSF V2 SP3. The initiatives are interdependent by design; ID02 generates OT visibility and intelligence, ID01 detects, investigates and responds using that intelligence, and ID09 governs and independently assures the effectiveness of both. This is further detailed in **Table 10** below.

Table 10: Summary of roles per layer

Program	Layer	Role
ID02	OT visibility	Generates OT asset intelligence, telemetry and vulnerability data that enterprise tools cannot produce natively
ID01	Enterprise operations	Detects, investigates and responds to threats using that intelligence across IT and OT
ID09	Governance & assurance	Governs cyber risk and independently assures the effectiveness of ID01, ID02 and the other seven programs

There is interdependence across the programs but not duplication. That several initiatives contribute to a common AESCSF outcome reflects the reality that mature control delivery requires governance, operational and technical capabilities working together; it does not mean the same capability, or the same expenditure, is funded twice. AusNet acknowledges the initial initiative descriptions could have more clearly articulated these boundaries and sets out the distinction in full below.

ID01 — Threat Detection and Response

Threat Detection and Response (ID01) enhances AusNet's existing enterprise cyber defence capability, delivering security monitoring and event correlation, threat intelligence and threat hunting, incident investigation and response, coordinated remediation, and security operations maturity. It provides the enterprise-level capability required to act on the OT intelligence generated by ID02. Without the proposed ID01 uplift, AusNet's existing enterprise capability would not provide the enhanced scale, coverage, detection engineering and response maturity required to operationalise the OT intelligence generated by ID02 and achieve the relevant SP3 outcomes

The AER's reduction to ID01 reflects a view that a shared solution could deliver both ID01 and ID02 more efficiently.

[C-I-C]

ID02 — OT Threat and Vulnerability Management

OT Threat and Vulnerability Management (ID02) delivers capabilities specific to operational technology environments: OT asset discovery and visibility, passive network monitoring, industrial asset intelligence, OT threat identification, OT vulnerability management, and engineering-led risk treatment. These address the safety, availability and operational requirements unique to OT and cannot be delivered through standard enterprise IT security tools.

[C-I-C]

The separation is shown in the **Table 11** below.

Table 11 - Summary capabilities between ID01 and ID02

Capability	ID01 Threat Detection & Response	ID02 OT Threat & Vulnerability Management
Enterprise Threat Detection	✓	✗
Security Incident Response	✓	✗
Threat Hunting	✓	✗
OT Asset Discovery	✗	✓
OT Protocol Analysis	✗	✓
OT Threat & Vulnerability Identification	✗	✓
OT Telemetry Generation	✗	✓
Enterprise Event Correlation	✓	✗

ID09 — Cyber Governance and Risk Management

The AER noted that AusNet already has cyber security governance arrangements in place and therefore considered additional governance investment unnecessary. AusNet agrees that foundational governance capabilities exist; however, [C-I-C].

AESCSF V2 SP3 requires a demonstrable enhancement beyond the SP1 baseline. The proposed Cyber Governance and Risk Management program (ID09) builds on existing governance arrangements

[C-I-C]

Table 12: [C-I-C]

These capabilities are not delivered through the proposed Threat Detection and Response (ID01) or OT Threat and Vulnerability Management (ID02) programs.

[C-I-C]

ID01, ID02 and ID09 operate at different layers; OT intelligence, enterprise detection and response, and governance and assurance and each delivers capability the others do not. Reducing scope across these programs would leave capability gaps that cannot be filled by the remaining initiatives and would prevent AusNet from achieving and sustaining AESCSF V2 SP3. AusNet maintains the original proposed scope and expenditure is required to reach the target capability outcomes.

2.5. Proposed phasing of ID05 and ID08 is required to enable dependent projects and AESCSF V2 SP3

The AER Draft Determination concluded that the proposed phasing of Data Protection (ID05) and OT Security Uplift (ID08) reflected delivery preference rather than the most prudent and efficient implementation pathway. On this basis, the AER adopted an alternative phasing approach, resulting in a reduction in forecast expenditure.

AusNet maintains the view that the proposed sequencing for both initiatives reflects capability dependencies rather than delivery convenience. Each phase establishes capabilities that are required to enable subsequent phases. Bringing later phases forward would increase implementation risk, create rework and reduce delivery efficiency, while delaying prerequisite phases would defer achievement of AESCSF V2 SP3 outcomes.

The rationale for the proposed sequencing is outlined below.

Proposed phasing of Data Protection (ID05) required to achieve AESCSF SP3

The AER's alternative phasing assumes that the components of the Data Protection program can be delivered independently or in a different sequence. AusNet considers the proposed sequencing to be the most prudent and efficient implementation pathway because each phase depends on capabilities established by the preceding phase.

The Data Protection program consists of three sequential phases:

[C-I-C]

The proposed sequencing reflects the logical progression required to implement effective and sustainable information protection controls.

[C-I-C]

[C-I-C]

Implementing the data protection capabilities before the underlying classification and protection controls are operational would reduce their effectiveness and create implementation inefficiencies.

Delivering the phases out of sequence would create implementation inefficiencies and duplicate effort. For example, deploying DLP policies before information assets are identified and classified would require subsequent redesign of classification labels, protection policies and monitoring rules. Similarly, implementing encryption and advanced protection controls before information ownership and classification are established would result in incomplete coverage and additional remediation activities. The proposed sequence therefore minimises rework, reduces implementation risk and represents the most efficient delivery pathway.

Accordingly, the proposed sequencing represents a prudent and efficient implementation pathway to achieve the intended AESCSF V2 SP3 in the coming regulatory period.

For these reasons, AusNet proposes to retain the original phasing of ID05.1, ID05.2 and ID05.3. The sequencing reflects the natural progression from identifying and classifying information, to implementing protection controls, and finally to applying advanced protection and privacy capabilities. This approach minimises implementation risk and provides the most efficient pathway to achieving the target maturity outcomes.

Proposed phasing of OT/IoT Security Uplift (ID08) required to achieve AESCSF SP3

The OT/IoT Security Uplift program (ID08) is the primary implementation program for establishing the OT security controls, infrastructure and operating capabilities required to achieve AESCSF V2 SP3 across AusNet's OT environment. The proposed sequencing reflects the progressive development of OT security capabilities, with each initiative enabling subsequent uplift activities.

The capability progression and intended outcomes are summarised in **Table 13** below.

Table 13: [C-I-C]

[C-I-C]

The proposed phasing reflects the practical sequence in which these capabilities can be implemented.

[C-I-C]

[C-I-C]

Accordingly, AusNet proposes to retain the original proposed OT/IoT Security Uplift (ID08) phasing and associated expenditure profile.

3. Recommendation

Recognising the AER's Draft Determination feedback, AusNet has completed review of the proposed cyber security program scope. This reassessment confirms that the nine non-recurrent programs proposed to reach AESCSF V2 SP3 perform distinct and complementary roles across architecture, implementation, operations and independent assurance from the control owner. While there are interactions and dependencies between some programs, these do not result in duplication of funded deliverables. In particular:

- Secure Software Development Lifecycle (ID06) addresses AESCSF V2 requirements for software security, software integrity, secure procurement, architecture review and security testing. [C-I-C]

- Identity Access and Management (ID03) and Defensible / Zero Trust Architecture (ID07) deliver distinct but complementary capabilities. ID03 implements enterprise identity, authentication, authorisation and privileged-access controls. ID07 defines the enterprise security architecture and implements the priority secure-access, device-trust, BYOD, trust-boundary and enterprise-segmentation controls required to realise that architecture. ID03 provides the underlying identity, authentication, entitlement and privileged-access capabilities consumed by those controls.
- Threat Detection and Response (ID01), OT Threat and Vulnerability Management (ID02), and Cyber Security Governance and Risk Management (ID09) perform separate operational, technical and assurance functions. ID01 operates enterprise cyber defence and monitoring services; ID02 establishes OT-specific threat, vulnerability, visibility and monitoring capabilities; and ID09 provides cyber risk governance, independent control assurance and compliance oversight.
- Data Protection (ID05) and OT/IoT Security Uplift (ID08) are deliberately phased to progressively establish the capabilities required for subsequent stages of uplift. The sequencing reflects the technical and control foundations needed to achieve the intended maturity outcomes, rather than a delivery preference.

Alternative delivery approaches were considered during review of the cyber security program. AusNet's reassessment confirms that the proposed scope and sequencing represent the most prudent and efficient pathway to achieving AESCSF V2 SP3 maturity in the coming regulatory period; maintaining appropriate cyber resilience for critical electricity infrastructure.

Collectively, the nine programs address the identified control effectiveness gaps, ASD Critical Infrastructure Uplift findings and AESCSF V2 practices required to be achieved. While individual practices may require contributions from multiple programs, each initiative delivers distinct capabilities and outcomes. Removal or material reduction of any program would leave control gaps unresolved and prevent full achievement of AESCSF V2 Security Profile 3.

AusNet therefore proposes the capex expenditure set out in **Table 15**, consistent with the initial proposal except for the accepted ID04 capex-to-open adjustment. All proposed expenditures represent transmission network allocation of AusNet total program costs, consistent with our Cost Allocation Methodology.

Table 15: Proposed total capex expenditure for Cyber Security program ($real 2025, Transmission allocated costs)

ID	Program name	Total
Non-recurrent expenditure to reach AESCSF V2 SP3 maturity *(made up of below)*		**$34.5m**
ID01	Threat Detection and Response	$7.7m
ID02	Operational Technology (OT) Threat and Vulnerability Management	$7.7m
ID03	Identity Access and Management	$6.2m
ID04	Cloud Security	$0.3m
ID05	Data protection	$3.5m
ID06	Secure Software Development Lifecycle	$2.1m
ID07	Defensible / Zero Trust Architecture	$2.9m
ID08	OT/IoT Security Uplift	$3.5m
ID09	Cyber Governance and Risk Management	$0.4m
Recurrent expenditure to maintain existing cyber security capabilities *(accepted in Draft Determination)*		**$20.4m**
Total Cyber Security Capex		**$54.9m**

AusNet

AusNet

Level 31
2 Southbank Boulevard
Southbank VIC 3006

T 1300 360 795

Locked Bag 14051
Melbourne City Mail Centre
Melbourne VIC 8001

Follow us on

@AusNet.Energy
@AusNet

ausnet.com.au