

E2E - Stage 2 options analysis (project initiation)

TN-Cyber Security Program of Work-Oct 22-(IES)

For work being proposed for inclusion into the capital works program.

Project name:	Cyber Security Program of Work (R24)
Department:	Technology & Performance
Investment Type:	Non-Network
Investment Category:	Non-Network – CAPEX and OPEX
Functional Area(s):	CYBRC: Cyber Security Capital Expenditure CYBRO: Cyber Security Operational Expenditure
Project ZoNe location:	<u>Cyber Strategy / R24 / IES</u>
Document Number:	<u>R24 IES S CS CYBRx Cyber Security V1.3.docx</u>
Needs Item Reference:	<u>R19-24 NEE S CS CYBRx Cyber Security.docx</u>
Regulatory Investment Test Required?	No
Version Number:	1.1
Date:	27/10/2022

Preferred Option:	Option 1				
Level 1 Estimate +/- 20 per cent ¹ (preferred option – base dollars):	\$8,129,240 CAPEX \$21,629,725 OPEX				
Expenditure profile	FY25	FY26	FY27	FY28	FY29
CAPEX	\$1,632,673	\$1,927,123	\$2,017,123	\$1,628,323	\$924,000
OPEX ²	\$2,827,890	\$4,154,215	\$4,807,790	\$4,908,540	\$4,931,290

Sign-offs (in support of the recommended option)			
Works Initiator:		Date	
Leader: (Endorsement)		Date	
Leader or General manager noting delegation levels. (Approval) ³		Date	

¹ Please note a 20% contingency has been used for the CAPEX amounts instead of the standard 30%. This is due to the detailed “bottom-up” approach used to estimate the investment required. A 30% contingency has been applied to the OPEX amounts.

² Includes forecasted overhead expense uplift to be incurred by the Cyber Security Team.

³ Approval based on delegation level.

1. RELATED DOCUMENTS

Description	URL
Needs Form	R19-24 NEE S CS CYBRx Cyber Security.docx
Estimate	Cost estimates R19-R24-R29 - risk mitigation V2.xlsx
NPV	R24 NPV S CS CYBRx Cyber Security (Finance review) V3.xlsx
Asset Management Plan	<i>Not applicable</i>
Cyber Security Strategy	Cyber Security Strategy for R24
TasNetworks Risk Appetite Statement (refer to page 12 “Infrastructure & Assets” and page 15 “Business Continuity Management” for cyber security risk specific content)	
TasNetworks Towards 2030 (refer to page 12 “Resilience” for an indirect cyber security reference)	
Future Distribution System Vision	
TasNetworks DRAFT 2021-22 Corporate Plan (refer to page 16 “Business Risks” and page 45 “Business Risks Details” for cyber security risk specific content)	
TasNetworks Three Year Business Plan 2021-2024 (refer to “Our Business” key performance indicators and “Intelligent Asset Management” focus area)	
TasNetworks Balanced Business Plan 2021-22 and TasNetworks Balanced Business Plan Handbook 2021-22 (refer to page 22 for the “Cyber Maturity Capability” measure and target)	
Technology & Performance Balanced Group Plan 2021-22	
TasNetworks Digital Strategy	
TasNetworks Risk Management Framework	
National Electricity Rules (NER)	
Australia’s Cyber Security Strategy 2020	
Security Legislation Amendment (Critical Infrastructure) Bill 2020	

2. OVERVIEW

2.1 APPROVAL GATE STATUS



Approval Gate	Approver Title	Approver Name	Date
Gate 1 – Needs	Leader Cyber Security	Steve Mason	23/08/2021
Gate 2 – Option	This project seeks OPTIONS APPROVAL to proceed		

In line with the Gated Investment Framework this Project seeks Gate 2 Option approval to proceed to budget and financial approvals. This IES presents economic and risk assessments for each option considered, together with recommendation of a preferred option to address the business need.

2.2 BACKGROUND

THE CYBER SECURITY THREAT LANDSCAPE

The cyber security threat landscape is rapidly changing characterised by an increasing volume of successful attacks both nationally and across the globe. The resilience of organisations' cyber security has also faced further changing demands due to the experiences with the COVID-19 pandemic and people working from home. This is further compounded by the change in the nature and sophistication of attacks.

Cyber threat actors are quickly adapting to these changing environments, and are quickly taking advantage of these new opportunities. This has seen a rise in both nation states and state-sponsored actors seeking political and economic advantage, plus financially motivated criminals operating like profit-driven organisations and successfully obtaining ransom due to targeted cyber-attack.

This challenges are exacerbated by an overwhelmingly complex technology stack and an increase in systems that were once in the deep underbelly of the organisation, such as Operational Technologies and Industrial Control Systems. Issues are further complicated by the challenges organisations face in finding and retaining skilled workers with specialist cyber security skills and qualifications. In its analysis of the top risks in the world, the World Economic Forum ranked cyber security failure in the top 10 risks by likelihood. As per Figure 1, cyber security failure is ranked high (>3.5 on a scale of 1 to 5) for both likelihood and impact.

The escalating cyber threat landscape can be attributed to the evolution, growth and increasing dependency on technology. This escalation of cyber threats in relation to the evolution of technology is represented in Figure 2.

2021 Global Risks Outlook

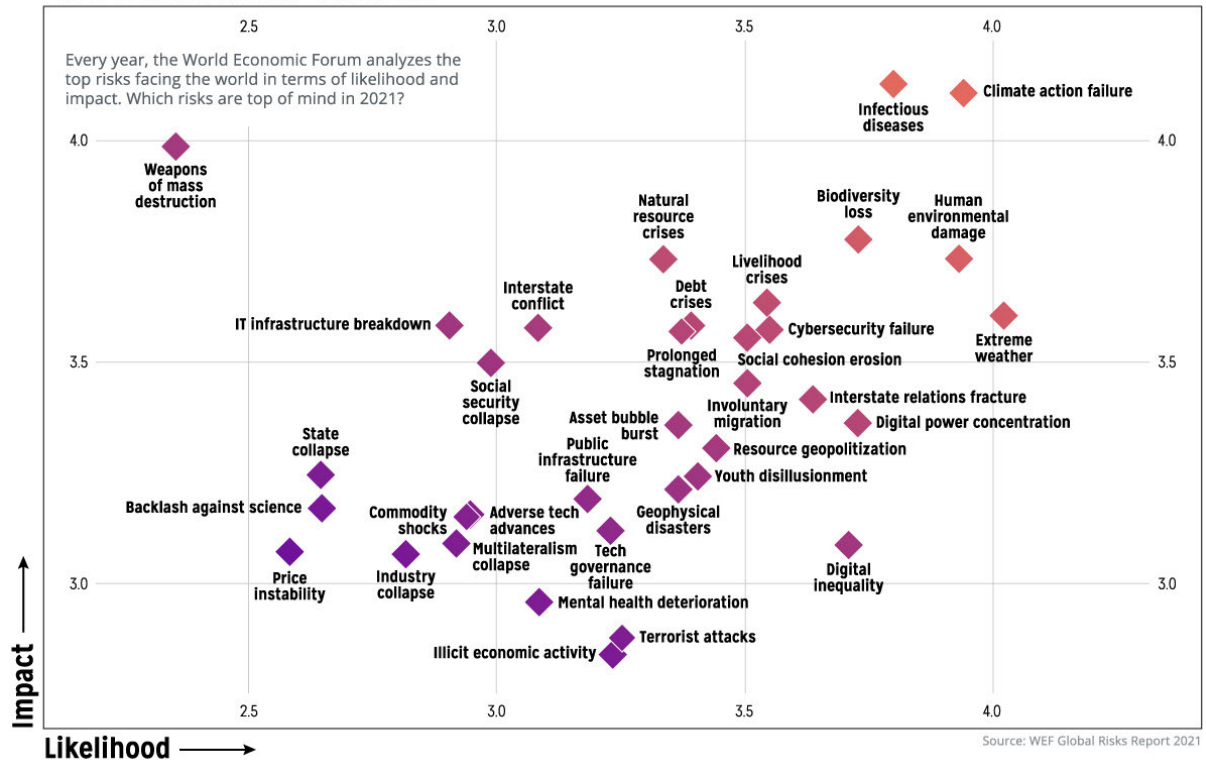


Figure 1: 2021 global risks outlook as per the World Economic Forum ⁴

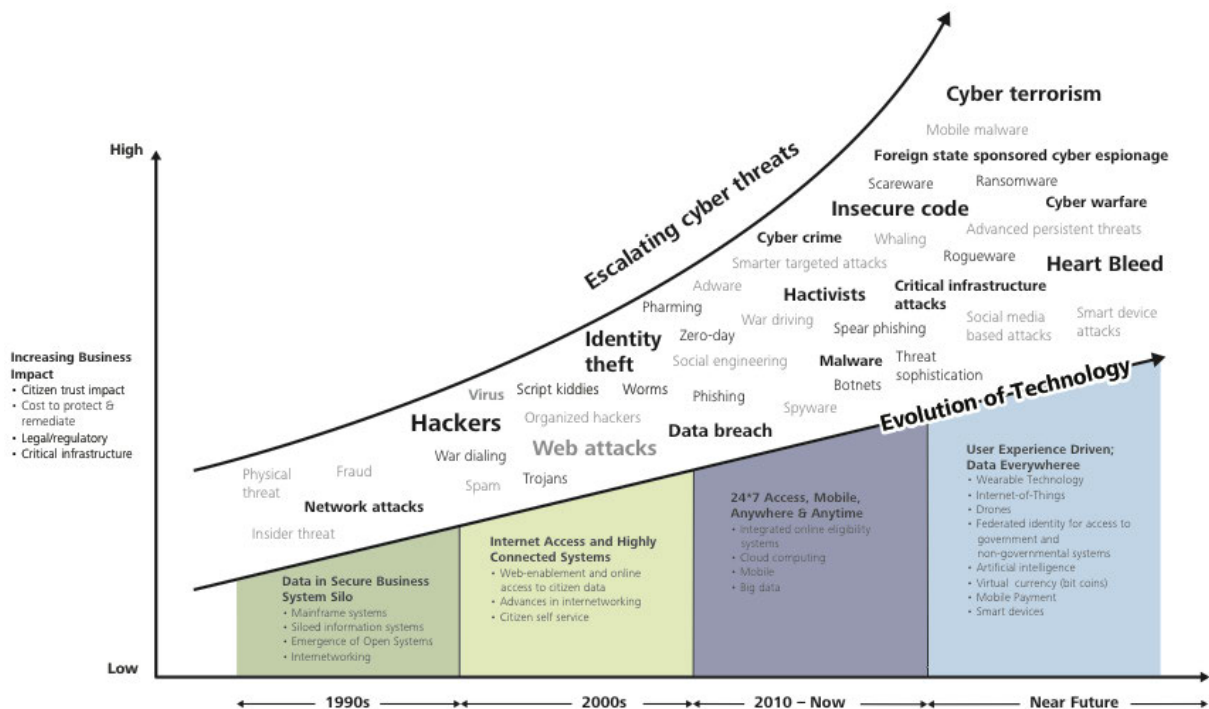


Figure 2: Relationship of rapidly escalating cyber threats with evolving technology ⁵

⁴ [Visualized: A Global Risk Assessment of 2021 And Beyond \(visualcapitalist.com\)](https://www.visualcapitalist.com/visualized-a-global-risk-assessment-of-2021-and-beyond/)

⁵ [2014 Deloitte - NASCIO cybersecurity study](https://www.deloitte.com/us/en/industry/financial-services/2014-nascio-cybersecurity-study.html)

The number of cyber security attacks within the electricity sector is rapidly increasing throughout the world, with a significant spike of incidents occurring in 2021. Figure 3 visually represents this concerning trend being experienced in our industry on a global scale.

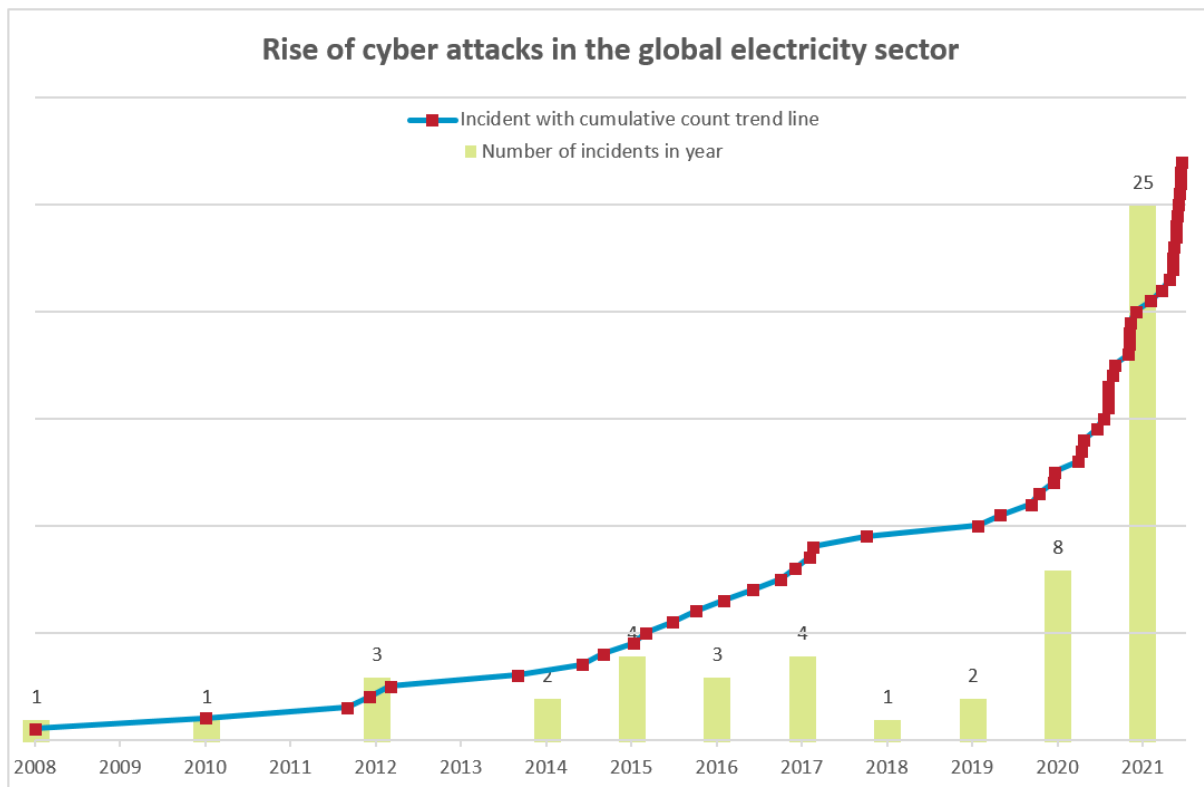


Figure 3: The risk of cyber security attacks being experienced globally within the electricity sector

The Australian Cyber Security Centre (ACSC) reported⁶ that between 1 July 2020 and 30 June 2021 they:

- Received over 67,500 cybercrime reports (which is an increase of nearly 13% from the previous financial year)
- The self-reported financial losses from cybercrime in Australia totalled more than \$33 billion, and
- Approximately one quarter of reported cyber security incidents affected entities associated with Australia's critical infrastructure.

This is supported by the Australian Government's Cyber Security Strategy 2020⁷ which outlines *cyber incidents targeting small, medium and large Australian businesses can cost the (Australian) economy up to \$29 billion per year, or 1.9% of Australia's gross domestic product (GDP).*

The ACSC also states there is *significant targeting, both domestically and globally, of essential services such as the health care, food distribution and energy sectors (which) has underscored the vulnerability of critical infrastructure to significant disruption in essential services, lost revenue and the potential of harm or loss of life.*

Some recent examples listed in Table 1 highlight the significant impact that cyber-attacks can have on businesses. Note this list focuses on significant cases known in 2020 and 2021. It doesn't include the multitude of cyber-attacks that have occurred before 2020.

⁶ [ACSC Annual Cyber Threat Report 2020-2021.](#)

⁷ [2020 Cyber Security Strategy \(homeaffairs.gov.au\)](#)

Table 1 Recent examples of cyber security attacks on businesses

Company	When	Impact
Spirit Super ⁸	May 2022	50,000 customer's information including names, addresses, ages, email addresses, phone numbers, super account numbers and the balances of members from the 2019-20 financial year were stolen after staff credential compromise .
Transport NSW ⁸	May 2022	An online application used by vehicle examiners to conduct roadworthiness inspections was attacked leading to data from "a small number of user accounts" stolen as a result of credential compromise .
South Australian Government	May 2022	90,000 South Australian public servants involved in payroll data breach perpetrated as a supply chain compromise of the state's payroll provider.
NDIS	May 2022	Successfully perpetrated supply chain compromise attack on NDIS from the cloud provider led to "A large volume of highly sensitive health data" stolen and posted on dark web forum.
AMD	May 2022	Weak passwords were the root cause that led to a successfully executed credential stuffing / brute force attack on AMD and saw the company lose 450GB of "sensitive" data.
Deakin University	July 2022	47,000 student details (PII) as a result of credential compromise of staff member's stolen credentials as a result of SMS phishing (smishing).
Victorian Government ⁸	July 2022	Successfully executed supply chain compromise attack saw personal data relating to travellers and staff, including names, contact numbers, dates of birth, addresses and passport information, was exposed following a privacy breach.
Woolworths	July 2022	An application vulnerability exists in Woolworths every day rewards app that allows an unauthenticated enumeration attack where anyone can enter a random card number and find a card's point balance. After entering the number in a rewards card app, the barcode can be produced, which can then be scanned at Woolworths checkouts to claim a discount
Marriott	July 2022	An attacker successfully executed a phishing attack lead to information of 400 staff members stolen.
Perth's Arts & Culture Trust	July 2022	Customers received notification of a successful supply chain compromise attack executed by attackers leading to "a massive data breach"
Cisco ⁸	August 2022	Cisco has revealed that it was hacked by a group affiliated with several well-known criminal groups, including Lapsus\$, UNC2447, and the Yanluowang ransomware gang from a Cisco employee's credential compromise
University of WA	August 2022	University of WA has suffered a credential stuffing / brute force attack that has led to PII and grades of current and past students being stolen
DoorDash ⁸	August 2022	Successful phishing attack of a supplier lead to supply-chain compromise of DoorDash leading to "an undisclosed" number of customer accounts stolen.
LastPass ⁸	August 2022	Attackers stole LastPass source code and "other sensitive data" as a result of a credential stuffing attack

⁸ Source: <https://www.webberinsurance.com.au/data-breaches-list>

Company	When	Impact
Optus ⁸	September 2022	An attack that led to exfiltration of 9.8 Million subscribers PII including passport and license information resulting from poor data governance, information and asset management processes that lead to customer data being accessible from the internet.
Telstra ⁸	October 2022	Data breach of a third-party provider resulting in a supply chain compromise attack leak of limited data of 30,000 current and former employees
Woolworths MyDeal ⁸	October 2022	Unauthorised access gained to the customer database of a website used by 2.2 million customers by an attacking using Compromised credentials
Medibank Private ⁸	October 2022	An attack resulting in contact from an actor wanting to negotiate regarding the unauthorised removal of 200GB of data including the personal information and medical diagnoses/procedures of customers
Energy Australia ⁸	October 2022	An attack on an the My Account online platform, resulting in the unauthorised access of customer data
Microsoft ⁸	October 2022	Misconfigured server exposed business transaction data between Microsoft and 65,000 prospective customers October 19, 2022
Australian Federal Police ⁸	October 2022	Over 5 million mails and tens of thousands of on live operations for Colombian and Australian agents working to stop drug cartels operating in Australia stolen in a breach October 14, 2022.
Vinomofo ⁸	October 2022	PII (name, address, contact information and D.O.B) from approximately 500,000 customers were stolen in a cyber-security breach

2.3 PROBLEM DEFINITION

STRATEGIC DRIVERS

From a National context: within the next decade, Tasmania forecasts generating up to twice the amount of electricity required by the state, with TasNetworks facilitating the delivery of this excess demand to other jurisdictions in Australia. This capacity is expected to be produced through a combination of windfarms and pumped hydroelectricity, driving the need for increased connectivity with the mainland.

As the nation's electricity grid becomes more interconnected and supply reliability more interdependent, AEMO will progress toward increased visibility of the electricity grid⁹. This increase in interconnectivity poses obvious supply chain risks to the grid generally, and requires further investment by TasNetworks to enhance and uplift the security posture of ICS/OT technologies that were never designed, nor intended to be externally accessible.

From a State context: TasNetworks electricity network needs to facilitate ongoing investment by individuals and businesses in photovoltaic and battery systems, while accommodating potential export of green hydrogen fuel¹⁰, increasing the demand for integration with Distributed Energy Resources and other yet to be defined resource providers. The requirement for these integrations further

⁹ <https://aemo.com.au/en/about/corporate-governance/corporate-plan>

¹⁰ <https://www.tasnetworks.com.au/config/getattachment/d513fd14-eca2-4848-9020-4651df59bebd/tasnetworks-towards-2030.pdf>

increases the TasNetworks attack surface, and exposes TasNetworks ICS/OT systems to external third and fourth parties.

From an Organisational Context: TasNetworks faces increasing pressure from stakeholders at all levels, including the general public and the Australian Energy Regulator (AER) to increase cost effectiveness that will contribute to placing downward pressure on end user bills for valued services¹¹. In response to this, TasNetworks will continue to identify and leverage opportunity to reduce total cost through strategic partnership. This value enhancement with potential cost reduction comes through business process and technology integration that increase TasNetworks' attack surface and exposes the organisation to a heightened level of threat of supply chain attacks.

TasNetworks plays an important role as the key link between electricity generators and electricity consumers for the state of Tasmania and exporting electricity to the rest of the nation. There is a natural consequence of this however, leading to an overall increase in the attack surface that TasNetworks presents. As a consequence, the period 2024-2029 presents a likely increased risk position for the organisation, requiring a security response.

The 2024-29 regulatory submission covered in this IES requires sufficient investment to maintain and secure the services provided by TasNetworks, while allowing the organisation to investigate novel ways of controlling cost.

TASNETWORKS' THREAT PROFILE

TasNetworks has recently reviewed and updated its threat profile and the aggregated cyber security risks that help inform the key business risk of a:

Successful attack against TasNetworks assets, leading to loss of control of the electricity network and/or loss of critical business system – impacting our ability to service customers, and/or maintain the confidentiality of information.

The current threat profile for TasNetworks considers the following threat actors:

- **Cyber criminals (including organised crime)** – with the primary intent of ransom or theft of sensitive data for profit
- **Hacktivist** – with the objective to cause reputational damage
- **Insider threats** – with a range of intents including theft of sensitive data, vandalism, deletion of data, accidental or deliberate misconfiguration and leakage of information and credentials
- **Nation state** – with a primary intent for theft of intellectual property, disruption of the power grid, and ongoing presence in the network.

Based on the intentions of these threat actors, TasNetworks considers the following cyber security risks to be particularly concerning and requiring attention:

- **Loss of control of the electricity network**, leading to system black/market suspension condition
- **Theft of sensitive information** leading to financial loss and reputational damage
- **Ransomware introduction** leading to widespread disruption of systems and services, theft and public exposure of sensitive information, *and*
- **Accidental loss of control of the electricity network**, leading to system black/market suspension condition.

Please refer to Appendix E – Aggregated Cyber Security Risks for the full list of aggregated cyber security risks.

¹¹ <https://www.energynetworks.com.au/resources/reports/electricity-network-transformation-roadmap-final-report/>

CYBER IMPERATIVE

As such, TasNetworks' Cyber Security imperative is to:

1. Respond to the identified strategic drivers; and,
2. Control current and perceived increase in threats, exposures and risks.

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

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

2.4 DELIVERY AND OBJECTIVES

TASNETWORKS' CYBER SECURITY JOURNEY

Since 2017, TasNetworks has embarked on a significant journey in the cyber security domain. On November 2017, the Board approved the TasNetworks Cyber Security Strategy as a whole-of-business strategy to proactively manage cyber security risks, its implications and associated compliance obligations. It stated as follows:

"The TasNetworks Cyber Security Strategy is to protect our critical assets – people, property and information – by establishing a contemporary enterprise-wide cyber security practice inclusive of human behaviour and technology-related threats and vulnerabilities."

Since the inception of this strategy, there have been numerous achievements made to improve our cyber security profile, including:

- 2017 – Update to the Cyber Security Strategy and the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and also the US Department of Energy's Cybersecurity Capability Maturity Model (C2M2);
- 2018 – The creation of cyber security function and the appointment of a Cyber Security Leader;
- 2018 – Establishment of a Cyber Security Program of Work to focus on an enterprise-wide risk-focused cyber security uplift;
- 2019 – Creation of a Cyber Security Governance Framework and cyber security-related policies, standards and procedures;
- 2020 – Appointment of new roles to compliment the cyber security function, including security architecture, risk analyst, security analysts and operational technology specialist;
- 2020 – Establishment of a Cyber Security Risk Management Strategy and the associated Top 10 Cyber Security Aggregated Risks; and

For the R19 revenue reset period, the focus for Cyber Security has been on establishing governance and undertaking discovery to understand the risks faced by TasNetworks. Activities included:

- Establishing the Cyber Security function;
- Development of governance artefacts (policies, standards and procedures);
- An increased understanding of the location, criticality, health and dependency of our technology assets;
- Identification of our key cyber security risks and appropriate mechanisms to protect ourselves from these risks; and
- Supporting the business to meet compliance obligations.

It is recommended this journey continues into R24 to uplift the cyber security capability and maturity as well as introduce efficiency improvements. The key themes for R24 include:

- Maintaining safe, reliable and secure delivery of Transmission and Distribution services;
- Enabling the organisation to successfully implement the business strategy securely;
- Uplifting the cyber security protection mechanisms;
- Increasing the transparency and reporting of cyber threats, risks and treatment actions;
- Automate and streamline cyber security operations; and
- Ensure there is long term sustainment and culture change.

Figure 4. provides a visual representation of TasNetworks' cyber security journey commencing in R19 and continuing through R24.

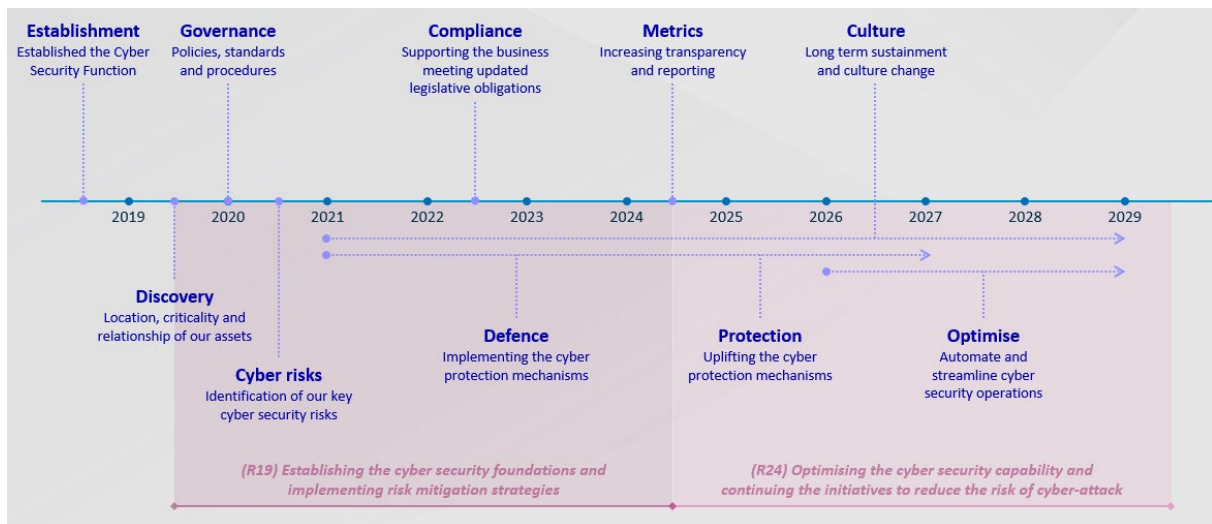


Figure 4: TasNetworks' cyber security journey

KEY THEMES FOR CYBER SECURITY IN R24

The following themes have been identified for the Cyber Security Program of Work in R24 to effectively identify, protect, detect, respond to and recover from cyber security threats and incidents:

- **Maintaining safe, reliable delivery of transmission and distribution services:**
 - Continue to roll out technology and process based solutions to mature the security of the systems that deliver electricity to the community and businesses in Tasmania, and to other jurisdictions of Australia
- **Enabling the organisation to successfully and securely implement the business strategy:**
 - Identify and implement enhancements, changes and optimisations in the current environment that are the required preconditions to the organisation achieving its strategic outcomes
- **Maintaining the risk of occurrence of cyber incidents that could result in operational impacts to TasNetworks including, but not limited to, data breach and loss of control at the current levels:**
 - Undertake active and ongoing monitoring of the threat landscape to protect from, detect and respond to concerns regarding our cyber security
- **Building capability to increase cyber maturity in line with recommendations for critical infrastructure service providers**
 - Supporting the growth in technology usage and reliance within TasNetworks and by our customers and stakeholders
 - Sustaining the cyber security function (people, processes and systems) and identifying opportunities for efficiency, automation and optimisation
- **Embedding cyber security practices across the organisation (embedding security by design) to prevent disruptions to business operations and/or loss of data:**
 - Increasing cyber security visibility within the organisation and reporting of cyber threats, risks and treatment actions
- **Transitioning cyber security awareness to long term sustainment and culture change:**
 - Increasing cyber security awareness and engagement including ongoing team member training and testing

CONCLUSION

The R24 investment period aims to mature the cyber capability implemented in previous regulatory periods, with a view maximising value from existing assets and any future procurement and through process maturation and evolution.

Doing so allows the organisation to achieve its strategic objectives, control risk, and progress implicitly toward [REDACTED] maturity posture.

3. CUSTOMER NEEDS AND IMPACT

The direct customers of Cyber Security are the internal partners and stakeholders across TasNetworks. Our external customers directly benefit from having more secure and resilient energy supply¹².

The internal stakeholders we have consulted with are listed in Table 2.

Table 2 Stakeholder consultation

Business function	Consult / Inform	Relationship
Network Operations Control Systems	Consult, at least weekly	Primary partner to improve cyber security within NOCS Consulted on the development of a plan to address the key cyber security risks applicable to their business unit
Telecommunication Networks Operations	Consult, at least weekly	Primary partner to improve cyber security within Telco Consulted on the development of a plan to address the key cyber security risks applicable to their business unit
Information Technology	Consult, at least weekly	Primary partner to improve cyber security within IT Consulted on the development of a plan to address the key cyber security risks applicable to their business unit
Asset Strategy & Performance	Consult, at least weekly	Primary partner to improve cyber security of secondary assets located within substations Consulted on the development of a plan to address the key cyber security risks applicable to their business unit Also consulted on the development of a plan to address the Physical Hazards Rules
Secondary Asset Engineering	Consult, monthly	Secondary partner to improve cyber security of secondary assets located within substations
Protection & Control (Field Operations)	Consult, monthly	Secondary partner to improve cyber security of secondary assets located within substations
Facilities	Consult, monthly	Consulted on the development of a plan to address the Physical Hazards Rules and general uplift of TasNetworks' physical security
Audit, Risk & Compliance	Consult, monthly	Primary partner to embed cyber security with the risk management framework Consulted on the development of a plan to address the Cyber Supply Chain Hazards and Material Risk Rules
Network Operations	Consult, quarterly	Consulted on the development of a plan to address the Natural Hazards Rules
People & Culture	Consult, quarterly	Primary partner to embed cyber security within workforce management Consulted on the development of a plan to address the Personnel Hazards Rules
Technical Capability	Consult, monthly	Primary partner to embed cyber security training and awareness with the workforce
Regulation	Consult, monthly	Understanding the impact of meeting the obligations associated with the Security Legislation Amendment
Revenue Reset	Consult, monthly	Preparing a submission for R24

¹² Refer to page 12 "Resilience" from *TasNetworks Towards 2030* document for an indirect cyber security reference.

Business function	Consult / Inform	Relationship
Finance	Consult, quarterly	Understanding the financial impact of treating risks and required OPEX step change
Legal Services	Inform, quarterly	Advised the potential requirement for a Privacy Management Plan (as per the AESCSF)

4. CORPORATE ALIGNMENT

4.1 BUSINESS PERFORMANCE OBJECTIVES

This project will help achieve the performance objectives outlined in the TasNetworks Three Year Business Plan 2021-2024 and the Technology & Performance Balanced Group Plan 2021-22, and as shown in Table 3.

Table 3 Performance objectives relevant to this project.

Performance category	Performance measure	Investment impact on performance
<i>Towards 2030</i> > Renewable Energy	<ul style="list-style-type: none"> • We play a pivotal role as catalyst for Tasmania's renewable energy economy, by connecting new customers and supporting emergent industries such as hydrogen production on Tasmanian soil. • We will enhance our processes and business capabilities to connect new large-scale renewable generation in Tasmania in a timely and skilful manner. • Work with governments, the community and other stakeholders to progress the design and approvals for Marinus Link. 	<p>The Project has direct impact on reconfiguring existing assets, deploying new assets, instantiating operating procedures, transitioning these to operations and executing the run activities necessary to securely integrate and enable Tasmania's renewable energy economy is dependent on TasNetworks integrating with energy generation, battery storage and, hydrogen production.</p> <p>The above also applies for integration with Marinus (subsidiary functional in its own right) to backhaul the energy to the mainland.</p>
<i>Towards 2030</i> > Resilience	Improving the resilience of our business by investing in prudent systems and processes, and deploying the right technology to allow us to make business decisions faster and safeguard our assets	Project has direct impact to ensure we're acquiring prudent systems and processes, and deploying the right technology to safeguard our assets (including people and information as well as physical assets)
<i>TasNetworks 3yr Business Plan</i> > Our Customers	<ul style="list-style-type: none"> • Being ready to connect and deliver power to the Bell Bay Advanced Manufacturing Zone (BBAMZ) for the production of renewable hydrogen in Tasmania, and • Building the capabilities to implement our Distribution Network Vision and Roadmap, enabling the participation of our customers in the renewable energy transition through the efficient integration of Distributed Energy Resources (DER). 	<p>The Project has direct impact on reconfiguring existing assets, deploying new assets, instantiating operating procedures, transitioning these to operations and executing the run activities necessary to securely integrate and enable Tasmania's renewable energy economy is dependent on TasNetworks integrating with energy generation, battery storage and, hydrogen production.</p> <p>The above also applies to Distribution Network Vision for efficient integration of Distributed Energy Resources.</p>
<i>TasNetworks 3yr Business Plan</i> > Transmission Readiness	• Maintaining our Transmission System Security	The project has a direct impact by enhancing vulnerability management, patch deployment testing, configuration management, audit and reporting of the ICS and OT systems.
<i>TasNetworks 3yr Business Plan</i> > Driving a Lean Business	<ul style="list-style-type: none"> • Live within our regulated operating expenditure allowances • Deliver the financial outcomes in our Corporate Plan • Allocation of finite resources to the right places 	The project has a direct impact on these measures as a result of identifying and executing automation of security capabilities where it makes commercial sense to do so, and by forecasting a realistic forecast of operational FTE required to maintain the security estate such that it maintains existing distribution and services, enables business strategic drivers without increasing risk while working towards increased maturity to SP-3 or equivalent.

4.2 RISK OBJECTIVES

The following statements in Table 4 are referenced from TasNetworks' Risk Appetite Statement (Infrastructure & Assets and Business Continuity Management):

Table 4 Relevant content from TasNetworks' Risk Appetite Statement

Sub-Category	Risk Appetite Statement	Risk Appetite
Safeguarding assets and systems	We have no appetite for unauthorised interruptions to the secure supply of electricity to our customers, including by compromising our physical security or corporate systems. Whilst risk and other vulnerabilities are present in all systems, risk-based approach must be adopted to reduce the risk to as low as reasonably practical.	No appetite
Business continuity	We have no appetite for a lack of implementation and testing of disaster recovery (DR), business continuity (BC) and other contingency plans for critical business processes.	No appetite
Cyber security and data protection	We have no appetite for failing to implement agreed risk-based cyber security strategies to deter, detect and respond to threats across all our systems, including our grid systems and related components, our control system, corporate systems and in the adoption of new technologies (e.g. smart meters).	No appetite
	We have no appetite for failing to implement agreed strategies to protect personal and sensitive information about our customers or commercially sensitive information about our business.	No appetite

This project will assist maintaining our current risk appetite and mitigating key business risks identified in TasNetworks' Corporate Plan. Table 5 presents all business risks, identifying those that would be positively impacted by the proposed project.

A detailed assessment of the risks mitigated by the project is presented in Section 5.

Table 5 Business risks mitigated by this project

Key Business Risks	Describe the specific risk(s) to which the business is currently exposed, for mitigation through the proposed project, and how it aligns with the Key Business Risk(s)
Death or Injury (Employee)	Project doesn't influence the management of this key business risk
Death or Injury (Public)	Project doesn't influence the management of this key business risk
Sustainable and Predictable Pricing	Project doesn't influence the management of this key business risk
Widespread Power Disruption	<i>(Project indirectly supports the mitigation of this risk)</i> Increasing TasNetworks' cyber security resilience can help reduce a causal factor that results in widespread disruption to the power supply leading to a black system condition or long-term load shedding (e.g. loss of control of industrial control systems). Refer to Project Objectives for mitigation strategies.
Bushfire Start	Project doesn't influence the management of this key business risk
Loss of Major Industrial	Project doesn't influence the management of this key business risk
Customer Focus	<i>(Project indirectly supports the mitigation of this risk)</i> Increasing TasNetworks' cyber security resilience can help reduce a causal factor that impacts on the customer experience (e.g. loss of control of industrial control systems). Refer to Project Objectives for mitigation strategies.

Key Business Risks	Describe the specific risk(s) to which the business is currently exposed, for mitigation through the proposed project, and how it aligns with the Key Business Risk(s)
Business Continuity Management	<p><i>(Project directly supports the management of this risk at the current and target level)</i></p> <p>Increasing TasNetworks' cyber security resilience can help reduce the likelihood and impact of a scenario where we are unable to continue to provide mission critical services at an acceptable level during an emergency, and recover to business as usual levels, or better, as soon as circumstances and resources allow (e.g. critical systems held to ransom).</p> <p>Refer to Project Objectives for mitigation strategies.</p>
[REDACTED]	[REDACTED]
Private Assets	Project doesn't influence the management of this key business risk
Energy Policy and Regulation	<p><i>(Project indirectly supports the mitigation of this risk)</i></p> <p>Non-compliance with the Security Legislation Amendment and Privacy Act will impact business revenue and reputation through financial penalties plus business information being disclosed publicly in court proceedings.</p>
Project Marinus (D&A)	Project doesn't influence the management of this key business risk
Tasmanian Power System Complexity	Project doesn't influence the management of this key business risk
Emerging Complexity of the NEM	Project doesn't influence the management of this key business risk

4.3 STRATEGIC OBJECTIVES

Table 6 summarises the strategic objectives that will be addressed by this project.

Table 6 Strategic objectives relevant to this project

Strategic Document	Strategic Objective	How the proposed investment will address the strategic goal
TasNetworks Digital Strategy	Protecting assets, data and reputation against the threats of the digital world, including cyber security	This is the primary objective of the project, to manage and mitigate cyber security risks to our assets, data and reputation
TasNetworks Towards 2030 <i>(Achieve efficiencies and reinvest gains in innovation for customers and growth)</i>	The regulatory construct is tightening to reduce prices for customers whilst managing transition	This is a primary objective of the project, to provide a secure technology platform the business can leverage to capitalise on innovation and reduce cost.
TasNetworks Towards 2030 <i>(Achieve efficiencies and reinvest gains in innovation for customers and growth)</i>	<ul style="list-style-type: none"> • We play a pivotal role as catalyst for Tasmania's renewable energy economy, by connecting new customers and supporting emergent industries such as hydrogen production on Tasmanian soil. • We will enhance our processes and business capabilities to connect new large-scale renewable generation in Tasmania in a timely and skilful manner 	This is a primary objective of the project, to enable the business to successfully execute its strategic objectives securely.
TasNetworks Towards 2030 <i>(Resilience of our network, our people and the community we serve)</i>	Building the resilience of our people and lifting our capabilities so we continue to adapt to new circumstances.	This is a primary objective of the project, with key initiatives focusing on workforce training, communication and awareness of cyber security risks and good practice
	Ensuring our electricity network remains resilient and fit-for-purpose by proactively maintaining it, designing out risks, and making prudent investments of long-term value.	This is a secondary objective of the project, to ensure "security by design" principles are considered with all our activities
	Improving the resilience of our business by investing in prudent systems and processes, and deploying the right technology to allow us to make business decisions faster and safeguard our assets.	Protecting / safeguarding our assets, including our information, is a primary objective of this project

5. PROJECT OBJECTIVES

This IES is an evolution of the **Cyber Security Program of Work** from R19 to R24 to support the business strategy securely and maintain the risk posture of the organisation, while maturing the Cyber Security function within TasNetworks toward [REDACTED]

In summary, the project objectives are as follows:

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

A range of initiatives have been identified to support the achievement of these project objectives. Further details about each of the proposed initiatives can be found in Appendix C – Option 1 Proposed Initiatives.

Please note that whilst this IES is focusing on the R24 revenue reset period (commences from FY2024-25 through to FY2028-29), initiatives and associated costings for the last two years of R19 (FY2022-23 and FY2023-24) have also been included for reference. This is due to the time of writing of this IES and that some of the identified initiatives transition from R19 into R24.

RISK MITIGATION OBJECTIVES

There are eight (8) aggregated cyber security risks that have recently been reviewed and assessed, that this IES aims to address, manage and mitigate. Please refer to Appendix E – Aggregated Cyber Security Risks for further details about these aggregated risks.

In summary, these eight aggregated risks are:

1. Loss of control of the electricity network, leading to system black/market suspension condition.
2. Theft of sensitive information leading to financial loss and reputational damage.
3. Ransomware introduction leading to widespread disruption and loss of system availability in IT environment.
4. Ransomware introduction leading to widespread disruption and loss of system availability OT environment.
5. Ransomware introduction leading to theft and public exposure of sensitive information.
6. Accidental loss of control of the electricity network, leading to system black/market suspension condition.
7. A network denial of service condition results in loss of telephony services and call centre availability.
8. Failure to adequately protect against cyber threats due to lack of comprehensive and trustworthy asset inventory and configuration management repository.

Table 7 outlines which initiative helps to address and mitigate specific aggregated risks.

Table 7 List of proposed initiatives to be delivered by the Cyber Security Program of Work

Initiative	Which risk(s) does it address?							
	1	2	3	4	5	6	7	8
ACSC Essential Eight Uplift	✓	✓	✓	✓	✓	✓	✓	
Asset Configuration and Change Management Uplift	✓	✓	✓	✓	✓	✓	✓	✓
Asset Identification & Vulnerability Management *	✓	✓	✓	✓	✓		✓	✓
Cloud Access Security Broker		✓			✓			
Cyber Security Capability Uplift	✓	✓	✓	✓	✓	✓	✓	✓
Data Loss Prevention		✓			✓			
Identity and Access Management Project (inclusive of Privilege Management)	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Threat Defence		✓	✓	✓	✓			
Monitoring, Alerting & Awareness *	✓	✓	✓	✓	✓	✓	✓	✓
Network Forensics	✓	✓	✓	✓	✓	✓	✓	
Security Architecture	✓	✓	✓	✓	✓	✓	✓	✓
Security Orchestration and Automation Response Project	✓	✓	✓	✓	✓		✓	
Threat Management *	✓		✓	✓	✓		✓	✓
User & Entity Behaviour Analytics	✓	✓	✓	✓	✓		✓	

* These initiatives will conclude their implementation phase in R19, however ongoing maintenance and further upgrades are planned for R24.

UPLIFT AND EMBED CYBER SECURITY CAPABILITY

The above-mentioned initiatives to be delivered via the Cyber Security Program of Work all support risk mitigation objectives and aid in uplifting and optimising the core cyber security services, being:

- Cyber Security Governance (Strategy, Policy, Compliance, Risk)
- Security Architecture
- Training, Awareness and Communication
- Management Reporting
- Auditing / Testing
- Cyber Security Technical Capability (with an enterprise focus), including:
 - Threat management
 - Vulnerability management
 - Monitoring & detection
 - Incident response

To ensure TasNetworks maintains and grows its cyber security capability and maturity, a number of additional roles have been identified. Please refer to Table 8 for further details. Also, please note the following:

- The yellow-highlighted rows indicate positions that are proposed to commence in R24, and
- The un-highlighted rows indicate positions that are proposed to commence in R19. These positions have been listed as the OPEX or team overhead allowances continue from R19 into R24 and have been included in the total R24 OPEX allowance request.

Table 8 Additional roles required to embed cyber security capability within TasNetworks

Identified position	FTE %	Proposed team	Proposed commencement date
Cyber Security Awareness & Engagement Specialist	1.0	Cyber Security	2022-23
Cyber Security Governance Specialist	1.0	Cyber Security	2022-23
Training Coordinator	0.4 ¹³	Cyber Security	2022-23
Threat & Vulnerability Management Role	1.0	Technology & Performance ¹⁴	2022-23
Technology Asset Configuration & Change Management (ACM) Officer	1.0	Technology & Performance ¹⁴	2022-23
Personnel Vetting Officer (for employees and contractors)	0.5	People & Culture	2023-24
Physical Security Officer	0.5	Procurement, Fleet & Facilities	2023-24
Support for Data Loss Prevention (DLP) e.g. data classification / ongoing support	0.3	IT Apps / Info & Records Mgt	2023-24
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹³ This role is currently funded as a 0.6 FTE and allocated to Learning Services. It is proposed this role is uplifted to 1.0 FTE by the indicated timeframe.

¹⁴ This role will need to work across Information Technology, Operational Technology (Network Operations Control Systems) and Telecommunication Services, all within the Technology & Performance Group.

6. OPTIONS ANALYSIS

6.1 OPTIONS CONSIDERED AND ECONOMIC ANALYSIS

Table 9 lists the options considered, the outcome of the economic analysis for each option, and the option being proposed for endorsement in this Investment Evaluation Summary. Details of the NPV analysis are included in Appendix A – Economic Analysis.

Table 9 Options considered

Option No.	Option summary	Direct cost (\$m)	NPV (\$m)	Preferred option (yes/no)	Reason for selection/rejection
0	Do nothing – This option includes maintaining the status quo and making no further investment to support cyber security risk mitigation	\$3.3m OPEX	(\$5.4m)	No	Making no further investment in cyber security puts TasNetworks at risk of cyber-attack, including ransomware and loss of critical systems
1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
2	This option includes all of Option 1, as well as the proposed initiatives at Appendix D – Option 2 Proposed Initiatives	\$26.5m CAPEX \$46.5m OPEX	(\$63.8m)	No	This option is a compliance-led security uplift for all capabilities, practices, processes and procedures uplifted to [REDACTED] irrespective of business drivers.

6.2 OPTION EXPENDITURE PROFILES

The following tables show the expenditure profile for each investment option. For further details please refer to the cost estimates which can be found [here](#).

Option 0 – Do nothing / maintain the status quo Estimate (in nominal dollars)					
Option 0 expenditure profile	FY25	FY26	FY27	FY28	FY29
CAPEX	-	-	-	-	-
OPEX	\$401,500	\$401,500	\$401,500	\$711,500	\$711,500

Please note Option 0 (do nothing) would require an uplift to the Cyber Security Team overhead expenses, if the seven existing FTEs aren't able to charge part of their time to contribute towards the proposed Cyber Security Program of Work for R24.

Option 1 – Focus on supporting organisation objectives while maintaining the risk position while attack surface is increased and attacks become more sophisticated. Estimate (in nominal dollars)					
Option 1 expenditure profile	FY25	FY26	FY27	FY28	FY29
CAPEX	\$1,632,673	\$1,927,123	\$2,017,123	\$1,628,323	\$924,000
OPEX	\$2,827,890	\$4,154,215	\$4,807,790	\$4,908,540	\$4,931,290

This IES supports a transition from predominantly CAPEX expenditure in the past, to a higher OPEX spend in the R24 Regulatory period. This is due to a number of underlying factors:

- As progress continues to a higher functioning, more mature cyber security capability within the business, implemented toolsets and functions such those to address vulnerability and threat management, and situational awareness are embedded. Subsequently, there is a shift to ongoing maintenance (including licencing and support) and enhancement of process and technology, beyond the initial implementation phase;
- Businesses are rapidly moving to more subscription based services, rather than perpetually licensed 'on-premises' capability (in large part due to the global IT market, with vendors moving away from offering on-premises options and only subscription based licensing). This shift also pertains to cyber security maturity uplift and results in a shift away from CAPEX procurement; and
- As cyber security capability grows, there is an increase expected in operational activity as opposed to program delivery, this results in a higher level of business-as-usual recurrent effort (primarily OPEX) in comparison to non-recurrent delivery effort usually related to project implementations (consisting of both CAPEX and OPEX).

Option 2 – Enhances Option to focus on reducing risk carried by the organisation Estimate (in nominal dollars)					
Option 2 expenditure profile	FY25	FY26	FY27	FY28	FY29
CAPEX	\$ 4,970,000	\$ 5,265,000	\$ 7,057,000	\$ 5,432,000	\$ 3,803,000
OPEX	\$ 6,877,000	\$ 8,504,000	\$ 9,307,000	\$ 10,458,000	\$ 11,381,000

Option 2 addresses the transformation projects and FTE uplift required by TasNetworks to reduce risk in the face of increasingly sophisticated attacks at a time when the organisation's attack surface is increasing.

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

And while the merit and value in executing these initiatives and reducing the overall risk position the organisation carries while allowing for automated attestation of technical controls and practices of the AESCSF, the cost to the community is deemed too great, and so this option has been determined as unbalanced. As such Option 2 is not the preferred option.

6.3 RISK MITIGATION

The matrix presented in Table 10 compares the options, showing how each assists TasNetworks in mitigating its key business risks (previously identified in Risk Objectives).

Appendix B – Key Business Risk Comparison provides supporting details of the risk assessment outcomes presented in Table 10.

Table 10 Risk matrix summary

Risk Drivers	Current Risk Position (Corporate Plan)	Option 0 – Do Nothing Maintaining the current profile will result in a worsening of the organisation's risk position due to increasing attack sophistication and the organisation increasing its attack surface	Option 1 – Balanced (preferred) Cyber security investment to compliment business strategy while maintaining current risk profile in the face of increased organisation attack surface and increasingly sophisticated attacks	Option 2 – Cyber-Led Outcomes Enhancement of Option 1 focused on reduce overall organisation risk and increasing maturity at the cost to the community and TasNetworks' customers
Cyber Security (KBR15)	■	■	■	■

6.4 QUANTITATIVE RISK ANALYSIS

Refer to:

- Appendix C – Option 1 Proposed Initiatives which identifies each initiative that will help address and mitigate the above risks;
- Appendix E – Aggregated Cyber Security Risks which summarises the aggregated cyber security risks (reviewed and updated September 2021); and

6.5 IMPLEMENTATION RISKS

Risks to implementation of the deliverables of each of the proposed initiatives exist and can be broadly identified in the following areas:

Table 11 Implementation Risks

Risk	Description
Technology	<p>The initiatives that form the scope of this IES are costed and scheduled based on the implementation of recommended existing technologies.</p> <p>The rate of change and complexity of new and advancing technologies is expected to have an impact on the scope, time and cost of several of the initiatives detailed within this IES.</p> <p>Whilst more appropriately addressing the solution requirements, the implementation of newer technology has a higher likelihood of presenting a greater level of risk; in vendor and product management, change management, user acceptance and of effective integration into the existing environment. All of these factors can lead to delays and other project impacts.</p>
Operational impacts	<p>Unplanned events (cyber incidents, impacts to business services, disaster events) may take precedence over the delivery of the initiatives detailed within this IES.</p> <p>Any influencing factors that impact the ability to resource the delivery of the projects identified, would require alternative planning.</p> <p>Due to the criticality of the need to deliver the initiatives that have been identified, scarcity of key resources may require the need to outsource components of project delivery, or to invest in external services.</p> <p>Any likely adverse event beyond the control of the project management is a potential risk. Such risks manifest in various types and forms, including storms, floods, bushfire, terrorism, vandalism, earthquakes and civil unrest. A project may stall or discontinue when such events occur.</p>
Skills Resourcing	<p>TasNetworks is operating cyber security as an in house function, with the requirement to retain close control of Intellectual Property for cyber security solutions.</p> <p>Leveraging on internal staff has the potential and likelihood to constitute a high risk as the ability to obtain and maintain the requisite level of specialist Cyber Security skills is an increasing challenge.</p> <p>Due to the limited market of cyber security specialists in Tasmania, the risk is increased in comparison to many other entities within the energy sector</p>
Evolving Scope Definition	<p>Any changes to intended initiative scope may lead to the extra cost of additional requirements, deliverables and outcomes to satisfy risk objectives and meet required business benefits.</p> <p>There are a number of influencing factors that could impact the scope of the initiatives that have been defined, including, but not limited to:</p> <ul style="list-style-type: none"> • Change and expansion to legislative obligations related to the ongoing updates to Security of Critical Infrastructure; and • Ongoing updates and strengthening of security requirements of frameworks measuring cyber security maturity; and • Modification of the business risk appetite.

6.6 BENCHMARKING

The Department of Home Affairs has undertaken a consultation and co-design process with TNSPs and DNSPs to understand the potential costs of introducing the Security Legislation Amendment, Governance Rules and Electricity Sector Specific Rules. These rules were designed in consultation with industry to effectively aid in the management and reduction of cyber security risk relevant to the energy sector.

The Department's draft Regulation Impact Statement¹⁵ outlined the average cost of compliance for each individual entity to manage / mitigate the risk of cyber-attack. Table 12 outlines this average cost and compares it with the cost estimate made by TasNetworks.

Table 12 Comparison of industry average cost of compliance with TasNetworks' estimates

Cost type	Industry average	TasNetworks' estimate
One-off	\$13.1 million	\$8.1 million
Ongoing (per annum)	\$4.6 million	\$4.3 million

¹⁵ Department of Home Affairs, Critical Infrastructure Centre – *Draft regulation impact statement: a risk management program framework for critical electricity assets* (6 August 2021).




6.7 PREFERRED OPTION

The preferred option is Option 1 as its objective is to deliver of a range of initiatives focusing on enabling the organisation's strategy while maintaining the current risk position (as outlined in Project Objectives) on the basis that option 1 represents best balance between cyber security outcomes, business enablement, and value for money for the community. A summary of the options analysis is displayed in Table 13 Preferred Option summary.

In contrast, Option 0 results in a regression of the overall security posture for the organisation as a consequence of broader integration of IT and OT systems because the current spend profile is outstripped by the increased sophistication of cyber-attacks, and the increased attack surface resulting from the organisation's business strategy to reduce cost of service, combined with regulatory requirements exposing the OT systems to an extent beyond what they were originally designed to cater for.

In conclusion, whilst option 2 delivers best of breed cyber outcomes while enabling regulatory requirements and business strategy execution, this reduced risk position comes at an increase in cost to Tasmanian consumers. On these grounds, option 2 has been deemed less suitable than a more balanced approach.

Table 13 Preferred Option summary

	Industry Average	Option 0	Option 1 Preferred	Option 2
Total CAPEX	\$13.1m	N/A	\$8.1m (38% below industry average)	\$26.5m (102% above industry average)
Total OPEX	\$23m	\$3.3m	\$21.6m (6% below industry average)	\$46.5m (102% above industry average)
Residual Risk Rating (aggregated)				
Contribution to Customer Outcomes		Low	High	Low

7. INVESTMENT TIMING

Table 14 summarises the delivery timeframes for each of the proposed initiatives found in Appendix C – Option 1 Proposed Initiatives

Please note the following:

- The yellow-highlighted rows indicate initiatives that are proposed to commence in R19 and continue through to the R24 revenue reset period
- The un-highlighted rows indicate initiatives that are proposed to commence and conclude in R24
- An OPEX step change will be requested to support the required uplift to mitigate the identified cyber security risks.

Table 14 Completion timeframes for each proposed initiative

	Indicative completion date (financial year)				
	2024-25				
	2024-25				
	2024-25				
	2025-26				
	2027-28				
	2028-29				
	2026-27				
	2026-27				
	2027-28				
	2027-28				
	2028-29				
TOTAL CAPEX (<i>indicative only</i>)	\$1.6m	\$1.9m	\$2.0m	\$1.6m	\$0.9m
TOTAL OPEX ¹⁶ (<i>indicative only</i>)	\$2.9m	\$4.1m	\$4.8m	\$4.9m	\$4.9m

Appendix F – Capital Expenditure Profile for R24 outlines the associated expenditure requirements for R24.

¹⁶ Includes forecasted overhead expense uplift to be incurred by the Cyber Security Team (above the currently budgeted amount of \$567k per annum).

8. EXPECTED OUTCOMES AND BENEFITS

The benefits to TasNetworks from implementation of the preferred option will be derived from the following key performance indicators:

- **Maintaining safe, reliable delivery of transmission and distribution services to meet TasNetworks Customer expectations**
 - Delivering a safe, reliable and dependable electricity supply to TasNetworks' customers in delivering Distribution and Transmission services in line with regulatory expectations and requirements
 - Enabling customers to have access to affordable and competitive electricity rates (through selection of pragmatic investment options)
 - Maintaining the security and privacy of customer details and privileged data
- **Enabling the organisation to successfully implement the business strategy securely**
 - TasNetworks' strategic vision is executed with a quantified risk position
- **Maintaining the risk of cyber incidents that could result in operational impacts to TasNetworks including, but not limited to, data breach and loss of control at the current levels**
 - TasNetworks risk position does not worsen over the regulatory period
- **Building capability to increase cyber maturity in line with recommendations for critical infrastructure service providers**
 - Enabling the business strategy and maintaining current risk posture sees TasNetworks explicitly and implicitly progress toward a [REDACTED] or equivalent
- **Embedding cyber security practices across the organisation (imbedding security by design) to prevent disruptions to business operations and/or loss of data**
 - Improved role definition and overall Identity management in order to simplify Role-based security, training and visibility
 - Increased visibility and information flow within the organisation of technical exposures, operational risks with enhanced management and improved tracking of treatment plans
 - Inclusion of risks, treatments and mitigations more systemically into the organisation's delivery plans
- **Transitioning cyber security awareness to long term sustainment and culture change**
 - Cyber training becomes further tailored and specific to the roles within the organisation

9. ASSUMPTIONS

The following assumptions are used to support this IES:

- A. A 20% contingency for CAPEX and a 30% contingency for OPEX has been applied to all cost estimates for the recommended option. Further, all cost estimates are in “today’s dollars” with no indexing applied.
- B. Contingency considerations include:
 - i. Changing obligations related to security of critical infrastructure are yet to be settled;
 - ii. Additional enhanced security obligations;
 - iii. Rate of change of new and emerging technology;
 - iv. Scarcity of, and competition for, appropriately skilled cyber security resources; and
 - v. Elevated and increasing cyber threat landscape, as evidenced by ACSC recommendations to adopt an enhanced security posture.
- C. A higher rate of OPEX contingency is allowed for in anticipation of:
 - i. Strong wages growth in conjunction with the need to attract and retain talented resources, particularly in the Tasmanian market where additional challenges and on-costs apply to engaging on the ground resources; and
 - ii. The higher likelihood that additional and heightened obligations for critical infrastructure entities will be applied during the R24 period.
- D. CAPEX contingency is set based on the expectation that in anticipation of further regulatory obligations, a portion of the CAPEX component is taking place prior to the commencement of the R24 period.
- E. Target cyber security maturity by the end of the existing R19 regulatory period [REDACTED]
[REDACTED]
- F. The current budget for the Cyber Security Team’s overhead expenses (\$567,442) will continue and receive a requested uplift (\$119,558) per annum from FY23. Therefore, all forecasted expenditure is only for the uplift required above and beyond this amount (\$687,000).
- G. Without a Cyber Security Program of Work (PoW) to partially allocate time to, the total budget for the Cyber Security Team’s overhead expenses would be \$1,225,000. This is included for Option 0 (*Do nothing / maintain the status quo*). Further details regarding Cyber Security resource forecast allocation to PoW vs operational activities can be found [here](#).
- H. Any investments required for information systems will be assigned a 10 year asset life with one major upgrade required around year 5.
- I. As the Program of Work implements technology and process driven solutions, an uplift in operational capability and personnel is required to maintain and support the enhanced cyber security function.
- J. It is appropriate for this IES to justify the additional roles required to embed cyber security capability within other teams and not just for the Cyber Security Team (as outlined in Table 8).
- K. Commensurate with current business risk appetite, Cyber Security is regarded as an in-house, sole sourced function. Any future change to this position would be managed within the identified OPEX budget.

10. REGULATORY INVESTMENT TEST

None of the options identified to address the business need exceed a direct capital expenditure cost of \$30m for R24, and therefore a Regulator Investment Test is not required.

11. RECOMMENDATION

It is recommended that the preferred option (Option 1) is approved and progressed, as it best satisfies the customer and business needs. The requested investment will enable TasNetworks to:

- Appropriately respond to and prevent the new emerging and ever evolving cyber security threats
- Maximise the current investment made to date to continue its cyber security maturity journey
- Support the increasing reliance on technology and services by instilling “security by design” principles
- Continue to meet our compliance obligations including the Security of Critical Infrastructure Legislation and Privacy Act, and
- Importantly reduce the overall risk and impact of cyber-attack to our business, customers and community.

APPENDIX A – ECONOMIC ANALYSIS

The assumptions used in the economic analysis are as follows:

- NPV analysis is carried out for a 10 year period (2024 to 2034).
- Real Weighted Average Cost of Capital (WACC) of 2.79 per cent is used.

The results of the Economic Analysis are provided below:

		Option 0	Option 1	Option 2
CASHFLOW	<i>flow</i>	Do nothing / maintain status quo	Cyber security business enablement	Business enablement and risk reduction
Capital Expenditure	Cash outflow	-	(11,309,240)	(29,177,000)
Operational Expenditure	Cash outflow	(6,185,000)	(45,148,675)	(70,045,950)
Operational Cost savings	Cash inflow	-	-	-
Total Expenditure	Cash outflow	(6,185,000)	(56,457,915)	(99,222,950)
Revenue	Cash inflow	-	-	-
Net Cashflow	Net cash	(6,185,000)	(56,457,915)	(99,222,950)
CASHFLOW NPV		(5,399,826)	(50,125,901)	(90,547,359)
PLUS NON CASH				
Non Cash Benefits	Non cash in	-	30,157,810	30,157,810
Non Cash Costs	Non cash out	-	-	-
Net Value	Net value	(6,185,000)	(26,300,105)	(69,065,140)
COST BENEFIT NPV		(5,399,826)	(23,402,341)	(63,823,799)
RANKING		3	1	2

APPENDIX B – KEY BUSINESS RISK COMPARISON

The project options each have a different impact on key business risks. Table 15 provides a qualitative summary of the impacts of each option on key business risks, with consideration for the risk approach and risk management process outlined in TasNetworks’ Risk Management Framework.

The backdrop for this assessment is best summarised as an increase in the overall risk position for TasNetworks of the regulatory period:

The attack surface for TasNetworks will increase within the regulatory period, as a consequence of both meeting regulatory obligations for integration and, as the organisation seeks innovation and competitive advantage to reduce cost to customers. Additionally, as the organisation increases its attack surface, the threat landscape is increasing as a result of economic pressures and increased sophistication of attacks. As such, over the regulatory period 2024-2029, TasNetworks will see an increase in its risk exposure.

Each of the options have the following implications on the expected, net risk position for TasNetworks:

- **Option 0 – Maintain – (Increase likelihood. Increase impact):** This approach proposes maintaining the current state of cyber security for the organisation, and as a consequence, TasNetworks will have a net increase in the risk exposure carried by the organisation.
- **Option 1 – Securely enable business strategy, maintaining current position and improving where feasible (Reduction in Likelihood. No Change impact):** Proposes to enable the organisation to achieve its strategy securely. Therefore, as the organisation increases its risk profile, the investment sought as part of this option will reduce the risk profile. The current risk position will be maintained throughout the regulatory period.
- **Option 2 – Significant investment in retrofitting organisation and proactive spend to reduce risk (reduction in likelihood. Reduction in Impact):** Proposes to enable the organisation to achieve its strategy securely and to focus on significant and material change that will execute systemic transformational change in the organisation, to execute an overall improvement in the net risk position of the organisation.

Table 15 Key Business Risk Option Comparison

Key business risks	Current risk as per Corporate Plan			Option 0 Maintaining the status quo and making no further investment				Option 1 Focusing on supporting organisation to deliver its strategic objectives without increasing risk position in the face of increasing attack surface and more sophisticated attacks.				Option 2 Enhancement to option 1 to include MIL3 maturity and risk reduction.			
	Likelihood	Consequence	Risk	Likelihood	Consequence	Risk	How does this option mitigate current situation risk?	Likelihood	Consequence	Risk	How does this option mitigate current situation risk?	Likelihood	Consequence	Risk	How does this option mitigate current situation risk?
Cyber Security	■	■	■	■	■	■	Option does not adequately protect the change in threat position and attack surface Maintaining the current level of investment will see an overall worsening of the security posture for the organisation. The net implication of this option is an increased risk to service delivery of power utility within Tasmania.	■	■	■	Option enables business strategy and reduces the likelihood of successful execution of cyber attack This option aims to secure the required technologies within the execution footprint of the organisation. The net implication of this option is the organisation strategy can be executed without increasing risk, while working towards reducing cost to consumers.	■	■	■	Option is focused on transforming organisation processes to be Cyber first, and to execute cyber capabilities proactively in anticipation of their use at a point in the future. This option faces significant barriers to execution across organisational change, capital expenditure and overall business interruption. The net implication of this approach will be an increased cost at the meter by customers.

APPENDIX C – OPTION 1 PROPOSED INITIATIVES

Table 16 details the proposed initiatives to be delivered by Option 1 for the Cyber Security Program of Work for R24.

Table 16 List of proposed initiatives to be delivered by the Cyber Security Program of Work aligned to AESCSF Domains

Initiative Title	Description	+	+	+	+	+	+	+	+	+	+	+
Legislative governance requirements (Sons)	If TasNetworks is declared a SoNS, this initiative is to address the following obligations: annual reporting, incident response planning, scenario-based exercising, vulnerability assessments, provision for access to information systems, etc.	X	X	X	X	X	X	X	X	X	X	X
ACSC Essential Eight Uplift	Support the attainment of [REDACTED] for all ACSC Essential Eight Maturity Model mitigation strategies, as per the draft Rules for the Data Sector.		X	X			X					
Asset Configuration and Change Management Uplift	Uplift of operational practices to [REDACTED]	X	X	X			X		X			
Asset Identification & Vulnerability Management (AIVM) - continuation	To enable TasNetworks to identify and manage cyber vulnerabilities affecting our connected assets, we must be confident that we have accurate, timely and detailed information about what assets are connected to our IT, OT, substations and telecommunications networks.	X	X	X					X			
Cloud Access Security Broker (CASB)	A system that sits between cloud service users and cloud applications, monitoring all activity and enforcing security policies.		X							X		
Cyber Security Capability Uplift	Capturing various activity across the business required to complete the uplift of Cyber Security Maturity in accordance with the AES-CSF framework. Many of the activities reflect coordination of effort across the business.	X	X	X	X	X	X	X	X	X	X	X
Data Loss Prevention (DLP) - continuation	To implement a range of technical and non-technical controls to reduce the likelihood of malicious and non-malicious data loss across the whole of TasNetworks.		X							X		X
Identity and Access Management Project (inclusive of Privilege Management)	Define and manage the roles (identities) and the related access of users and devices to all of our on-premises and cloud applications. Cover the entire lifecycle of on-boarding, managing authorisations and off-boarding in a timely manner.	X	X	X	X					X		
Mobile Threat Defence	Protecting TasNetworks portable devices (Laptops, Mobile Phones, and Tablets) from malware and phishing, detecting device level vulnerabilities & insecure configurations, providing security hygiene and monitoring for suspicious activity.		X			X		X		X		

Initiative Title	Description	+	+	+	+	+	+	+	+	+	+	+
Monitoring, Alerting & Awareness	An initiative to coordinate and direct effort within the Cyber BAU team and among various stakeholders focusing on: <ul style="list-style-type: none"> • Risk Based Alerting • Enhancing Situational Awareness • Ongoing Continuous Improvement of Logging & Monitoring 		X	X		X		X	X			
Network Forensics	To create an ongoing set of securely stored network packet data to enable the full reconstruction of cyber security incident. This project will produce what will be equivalent to an aircraft black box which can only be accessed by authorised users to reconstruct a cyber security incident. Network data will enable incident traceability and is critical in enabling the business to recover from such a cyber security incident.		X			X	X	X	X			
Security Architecture	Develop a comprehensive, structured approach to selecting appropriate security processes, systems and controls across the enterprise. This will require particular focus on the network control systems and operational networks, acknowledging the unique constraints within those environments.	X	X	X	X	X	X	X	X	X	X	X
Security Orchestration and Automation Response (SOAR) Project	Respond to security events with minimal human interaction. Connect internal and external tools via built-in or custom integrations and APIs, then use the corresponding data to create repeatable, automated processes to replace existing manual processes. — where event analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardised response activities.		X			X	X	X	X			
Threat Management	Build systems to ingest evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about existing or emerging hazards. This project will select threat intelligence sources and feeds, as well as building a system to ingest them and enrich the		X	X		X	X	X	X			
User & Entity Behaviour Analytics	Uses Machine Learning and Deep Learning to model the behaviour of users and endpoints to detect complex attacks by building a pattern of normal behaviour and detecting anomalies.		X			X	X	X	X			

APPENDIX D – OPTION 2 PROPOSED INITIATIVES

Table 17 below details the proposed initiatives for Option 2. Option 2 includes all activities from Option 1, as well as enhancements for establishing and maintaining automated operating effectiveness for key MIL-3 controls and practices.

Successful execution of Option 2 will result in an overall risk reduction for TasNetworks with the net effect of higher costs of utilities for the community and consumers of TasNetworks services.

While this option is most assuredly the better option from a cyber-security perspective, it does not represent the most balanced value for money, and as such is not the preferred option.

Table 17 Proposed Initiatives Option 2

Initiative Name	Brief Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Initiative Name	Brief Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

APPENDIX E – AGGREGATED CYBER SECURITY RISKS

Table 18 summarises the aggregated cyber security risks that were reviewed and updated September 2021. For further details regarding these aggregated cyber security risks please contact the Cyber Security Risk Analyst within the Cyber Security Team.

Table 18 List of proposed initiatives to be delivered by the Cyber Security Program of Work

ID	Risk title	Threat actor(s)	Risk rating
1	Loss of control of the electricity network, leading to system black/market suspension condition.	Nation State Cyber Criminal Insider Threat	■
2	Theft of sensitive information leading to financial loss and reputational damage.	Nation State Insider Threat Hacktivist	■
3	Ransomware introduction leading to widespread disruption and loss of system availability in IT environment.	Nation State Cyber Criminal Hacktivist	■■■
4	Ransomware introduction leading to widespread disruption and loss of system availability OT environment.	Nation State Cyber Criminal Hacktivist	■■■
5	Ransomware introduction leading to theft and public exposure of sensitive information.	Nation State Cyber Criminal Hacktivist	■
6	Accidental loss of control of the electricity network, leading to system black/market suspension condition.	Insider Threat	■
7	A network denial of service condition results in loss of telephony services and call centre availability	Cyber Criminal Hacktivist	■■■
8	Failure to adequately protect against cyber threats due to lack of comprehensive and trustworthy asset inventory and configuration management repository.	All	■

APPENDIX F – CAPITAL EXPENDITURE PROFILE FOR R24

Table 19 is an extract of the full expenditure profile which focuses on the capital expenditure for the R24 period for Option 1.

Table 19 List of proposed initiatives to be delivered by the Cyber Security Program of Work

Initiative	FY25	FY26	FY27	FY28	FY29	SUBTOTAL
[REDACTED]	\$-	\$-	\$-	\$180,000	\$180,000	\$360,000
[REDACTED]	\$150,000	\$-	\$-	\$-	\$240,000	\$390,000
[REDACTED]	\$300,000	\$300,000	\$-	\$-	\$-	\$600,000
[REDACTED]	\$-	\$200,000	\$200,000	\$200,000	\$-	\$600,000
[REDACTED]	\$93,000	\$93,000	\$93,000	\$-	\$-	\$279,000
[REDACTED]	\$80,000	\$-	\$-	\$-	\$-	\$80,000
[REDACTED]	\$-	\$145,800	\$145,800	\$-	\$-	\$291,600
[REDACTED]	\$-	\$-	\$300,000	\$300,000	\$300,000	\$900,000
[REDACTED]	\$-	\$390,000	\$390,000	\$-	\$-	\$780,000
[REDACTED]	\$483,323	\$564,323	\$564,323	\$564,323	\$-	\$2,176,290
[REDACTED]	\$30,000	\$30,000	\$-	\$60,000	\$-	\$120,000
[REDACTED]	\$292,350	\$-	\$-	\$-	\$-	\$292,350
[REDACTED]	\$204,000	\$204,000	\$204,000	\$204,000	\$204,000	\$1,020,000
[REDACTED]	\$-	\$-	\$120,000	\$120,000	\$-	\$240,000
TOTALS (per annum)	\$1,632,673	\$1,927,123	\$2,017,123	\$1,628,323	\$924,000	\$8,129,240

Please note that some of the later expenditure indicated in FY2028 and FY2029 may represent forecasted technology upgrades.