# IT Security

| | |
|---|---|
| **Project name:** | Security |
| **Department** | Technology and Performance |
| **Investment Category** | Information technology (support the business) non-network |
| **Network** | Shared |
| **Project ND number / work category:** | ITC |
| **Project Zone location:** | R0000736246 on the Project Zone |
| **Document number:** | 1958 |
| **Version number:** | 1 |
| **Date:** | 22/11/2018 |
| **Project initiation approval reference:** | R0000748131 |

| **Preferred Option:** | | | Option 1 | | |
|---|---|---|---|---|---|
| **Estimate (preferred option – base dollars):** | | | [redacted] | | |
| **Expenditure profile** | **19/20** | **20/21** | **21/22** | **22/23** | **23/24** |
| Capex | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Opex | | | | | |

| **Sign-offs (in support of the recommended option)** | | | |
|---|---|---|---|
| Project Initiator: | [redacted] | Date | 22/11/2018 |
| Leader:<br>(Endorsement) | [redacted] | Date | 22/11/2018 |
| Leader or General manager noting delegation levels.<br>(Approval)[1] | [redacted] | Date | 22/11/2018 |

[1] Approval based on delegation level.

# 1. Overview

## 1.1 Background

Effective security in both IT and OT domains is essential to safe and reliable operation of the network. Execution of the planned program and operational activities will enable TasNetworks to ensure safe and reliable energy supply, maintain compliance with license conditions and enable continued compliance with regulatory requirements for data privacy.

This Investment Evaluation Summary (IES) documents planned expenditures for the determination period for items that cover systems positioned within both the OT and IT environment responsible for inspecting, auditing and restricting system interactions (security systems).

At a high level the scope consists of activities that reduce risk and exposure and improve TasNetworks cyber security posture and capability through:

- Improvement in TasNetworks implementation of Australian Signals Directorate Cyber Security recommendations
- Improvement in TasNetworks maturity level against the Australian Energy Sector Cyber Security Framework
- Improvements to device security (including servers, client and mobile devices)
- Enhancement of network perimeter and interior security measures
- Increased application security
- Appropriate configuration and control or remote access to TasNetworks IT facilities
- Enhancements to IT and OT Security management, risk and governance processes
- Increase Cyber Security awareness and education of staff

Arising from the Finkel 2.10 review covering cyber security protection of the National Electricity Network, and the subsequent development of the Australian Energy Sector Cyber Security Framework (AESCSF) by AEMO, TasNetworks recently undertook assessment as part of an AEMO investigation into the cyber security maturity of energy market operators. The assessment provided both a current state and (based on AEMO expected recommendations) a target-state position for TasNetworks.

Based on the assessment results, TasNetworks has developed a capital expenditure program of work designed to lift TasNetworks maturity levels in order to:

- Address recommendation 2.10 of the Finkel Review, whereby requirements to implement AESCSF (formerly ES-C2M2) is advised
- Attain and maintain AESCSF Maturity Implementation Level 3 across all applicable domains in the Regulatory Period
- Address Australian Signals Directorate recommendations that organisations comply with mitigation strategies.

These additional program of work items have been assessed against the original IES numbers to ensure there is no duplication within the existing IES submission.

Additional expenditure required to address the targeted AEMO AESCSF maturity levels covers the following activities:

- Explicit compliance against the Australian Signals Directorate mitigation strategies
- Uplift of Asset and Configuration Management processes and controls
- Significant development of Governance, Policies and Procedures
- Delivery of improved Threat and Vulnerability Management capabilities across the Operational Technology Landscape
- Improvements to Physical Access Controls across assets and sites
- Improvements to Substation device and network security implementation.

Security is essential to the safe operation of the network. Increasing levels of sophistication are being brought to bear against targets, with our industry seeing a much higher level of targeting than industry standards.

## 1.2 Problem Definition

TasNetworks ability to prevent, detect and respond to cyber security incidents and breaches does not currently meet recommended practices documented in the AESCSF. Additionally, work is needed to improve implementation of Australian Signals Directorate mitigation strategies to better protect TasNetwork IT and OT systems and reduce both the likelihood and severity of cyber security incidents.

Improvements to TasNetworks cyber security processes enables:

1. Reliable and effective delivery of IT services to the TasNetworks business and external customers.
2. Compliance with state and federal legislative and regulatory requirements, including:
    a. Industry-specific requirements.
    b. State and federal privacy legislation.
    c. Occupational Health and Safety requirements.
3. Maximised efficiency, flexibility and cost-effectiveness of service delivery.

Activities driving the requirement for capital expenditure in this IES are documented in *the TasNetworks Cyber Security* Strategy and *IT Infrastructure Asset Management Plan*. To summarise, these activities will consist of:

- Operational support and maintenance of the platform infrastructure
- Risk reduction and exposure mitigation
- Ability to extend capability as required.

These activities will allow TasNetworks to maintain reliable and efficient infrastructure in support of safe delivery of energy to customers.

# 2. Customer needs & impact

TasNetworks' cyber infrastructure is critical to the reliable, timely and effective delivery of application and data services to staff, customers and network operation. These services are directly related to TasNetworks' ability to deliver efficient and effective services to our internal and external customers. The management of the items in this IES are critical to the operation of these components.

Failure of cyber security systems can lead to severe adverse consequences to TasNetworks and customers, including:

- Loss of supply (for example, breach of the Ukrainian power grid in 2016 saw loss of supply to 225,000 customers for almost six hours)
- Loss of revenue (hacking of smart power meters in Puerto Rico in 2019/2010 cost the controlling utility an estimates US$400M in lost revenue)
- Damage or destruction of assets (for example, the StuxNet attack destroyed over 900 uranium enrichment centrifuges in 2010)
- Unauthorised access to and dissemination of personally identifiable information (examples include the PageUp data breach in 2018)

Security measures must continue to protect TasNetworks IT and OT networks, while adapting to a changing threat landscape that is increasing in sophistication.

TasNetworks is strongly focussed on service delivery to customers. These services are delivered in a manner that aligns with TasNetworks' mission, commitments and values. The customer consultation program for the Program of Work documented in this IES reflects an approach of constant and direct engagement with business customers through:

- Regular direct meetings with management teams from all business units at least every six months
- Alignment with the TasNetworks Risk Framework and Cyber Security Strategy
- A formal project prioritisation process that includes full transparency, extensive customer consultation and business-determined priorities
- A fully consultative project management methodology that embeds TasNetworks customers in every stage of the project.

# 3. Corporate alignment

## 3.1 Strategy objectives

The following table highlights how the initiative will assist in achieving TasNetworks' Strategy for 2025.

**Table 1 Strategic Goals relevant to this project**

| Strategic Goal | How this initiative will address the strategic goal |
|---|---|
| **Business Productivity** – "Optimise our program of work and emergency response capability delivering on our promise" | • Continued availability of IT and OT systems underpinning service delivery to customers. |
| **Network Capability** – "Our network continues to meet demand and power system security systems requirements while accommodating the changing use of our network" | • Reduction or prevention of supply interruptions arising from breach of the OT network |

## 3.2 Performance objective

This project will help to achieve the customer and business performance objectives in TasNetworks' Corporate Plan 2017-18 to 2023-24 and aligns with the 2019 to 2024 regulatory period. The relevant performance indicators and measures are presented in table 2.

**Table 2 Performance objectives relevant to this project**

| Performance measure | Measure | Project objective |
|---|---|---|
| Zero harm | Number of significant incidents | Prevent incidents arising through breach of OT systems |
| Sustained cost reduction | Efficient operating and capital expenditure. | Reduce likelihood and impact of breach of both IT and OT systems |
| People | Staff turn over, engagement scores | Reduce likelihood and impact of breach of both IT and OT systems |
| Customers | Customer net promoter score | Reduce likelihood and impact of breach of both IT and OT systems |
| Network service | Transmission loss of supply events | Prevent loss of supply events arising through breach of OT systems |

## 3.3 Risk objectives

The corporate plan identifies a number of business risks outlined in the TasNetworks Risk Framework[2], which details the level of risk the business finds acceptable in each category (Safety, Environmental, Financial, Regulatory, Legal and Compliance, Customers, Assets, Reputation and People).

This initiative addresses People, Financial, reputation and compliance risks, of which TasNetworks has a [redacted] to [redacted] appetite.

Those risks, which will be impacted by this project, are presented in table 3.

**Table 3 Risks impacted by this project**

| Key Risk | Consequence | Likelihood | Rating | Impact |
|---|---|---|---|---|
| Failure to address key business cyber security risk | SEVERE | LIKELY | CRITICAL | • Breaches of regulatory or legal obligations<br>• Fraud Implications<br>• Loss of data and/or loss of business system functionality<br>• Loss of data or reputation from employee opening malware/ransomware or other malicious software via email<br>• Loss of visibility and control of the power system<br>• Physical asset damage<br>• Significant business interruptions |

[2] ZoNe ref. R0000238142.

| Key Risk | Consequence | Likelihood | Rating | Impact |
|---|---|---|---|---|
| Targeted attack resulting in a compromise of the power network | SEVERE | UNLIKELY | HIGH | • Injury or Illness that results in fatality or permanent impairment<br>• Material supply interruption to 25,000 to 75,000 distribution customers<br>• Damage to transmission, distribution or customer assets due to quality of supplier<br>• Impact to or loss of one major industrial customer<br>• Non sustained state-wide press coverage<br>• Industrial action<br>• Local community complaints |
| Breach of market operator compliance requirements | MODERATE | ALMOST CERTAIN | HIGH | • Sustained regulated attention on operations with potential for external investigation<br>• Non sustained state-wide press coverage |
| Disclosure of private and/or confidential information | MODERATE | LIKELY | HIGH | • Minor systemic breach of regulatory compliance requirements<br>• Non sustained state press coverage<br>• Industrial action preventing delivery of service to customers |

# 4. Project objectives

The primary objective of this initiative is to ensure the continued availability and integrity of TasNetworks IT and OT systems. Meeting the objective will contribute to continued safe and reliable delivery of supply and other services to TasNetworks customers as well as meet legislative, regulatory and licensing conditions applicable to TasNetworks.

This objective is achieved through meeting the following initiative objectives:

1. Provide sufficient isolation and control of traffic between security zones including:
    a. Corporate to internet interface
    b. Corporate to operational network interface
    c. Inter security zones within the larger Corporate zone
    d. Business to business interfaces.
2. Ensure that services are operated to meet TasNetworks' compliance requirements for data privacy and data retention.
3. Ensure that all security facilities are:
    a. Licensed, and installed in compliance with vendor license requirements
    b. Supported by the vendor to a level appropriate to IT service level objectives
    c. Upgraded or replaced as necessary to meet the requirements above.
4. Ensure replacement of security hardware and software in line with the IT Infrastructure Lifecycle policy to meet the investment needs documented above.
5. Provide a platform to meet IT service level requirements through the determination period.
6. Provide sufficient performance of the services over the period.
7. Ensure that the availability of services meets or exceeds IT service level targets through appropriate configuration and procurement of suitable support agreements.
8. Ensure services are flexible to cater for changing landscape.

The objectives will be met through the execution of implementation, maintenance, upgrade, extension and replacement activities as described.

# 5. Revenue Determination

N/A

# 6. Options analysis

Each option has been selected and assessed with regard to the following criteria:

1. **Solution effectiveness:** solution effectiveness is tested against the problem (detailed in chapter 1.2 titled "Problem Definition");
2. **Cost** (estimates used on the analysis have a level of accuracy of ±30% and do not include the 20% project contingency normally applied to this type of project);
3. **Business impact:** the selected option will consider the level of change to TasNetworks environment (including during project implementation and post implementation);
4. **Business Strategic alignment:** does the option fulfil the business objectives and current business initiatives (detailed in chapter titled "Corporate Alignment");
5. **Information Technology Strategic alignment**;
6. **Project complexity:** solutions have the minimum level of complexity needed to meet the business requirements;
7. **Risk profile:** solutions will be risk averse;
8. **Compliance:** ability to achieve compliance. Solutions will be fully compliant with all regulatory requirements and applicable industry standards;
9. **Time:** solutions will be implemented within a suitable timeframe to ensure compliance (where relevant), minimise disruption to the business and reduce the likelihood of project requirements becoming dated.

The following table compares the options presented with regard to the criteria assessed in the previous chapter.

**Table 4 Summary of Drivers**

| Driver | Option 0<br>Do Nothing | Option 1<br>Improve Cyber Security Capability |
|---|---|---|
| 1. Solution effectiveness | | |
| 2. Cost | | |
| 3. Business Impact | | |
| 4. Business strategic alignment | | |
| 5. IT strategic alignment | | |
| 6. Project complexity | N/A | |

| | | |
|---|---|---|
| 7. Risk profile | | |
| 8. Compliance | | |
| 9. Time | N/A | |

The table below shows the key for each rating.

**Table 5 Drivers Rating Key**

| Driver | Rating 1 - Green | Rating 2 - Yellow | Rating 3 - Red |
|---|---|---|---|
| Solution effectiveness | Addresses most requirements | Addresses some requirements | Addresses few requirements |
| Cost | Low | Medium | High |
| Business Impact | Low | Medium | High |
| Business strategic alignment | Good alignment | Partial alignment | Poor alignment |
| IT strategic alignment | Good alignment | Partial alignment | Poor alignment |
| Project complexity | Low | Medium | High |
| Risk profile | Low | Medium | High |
| Compliance | Easy | Moderate | Hard |
| Time | Easy | Moderate | Hard |

## 6.1 Options considered

The following table lists the options considered.

**Table 6 Options considered for this project**

| Option No. | Option description |
|---|---|
| 0 | Do nothing, allowing existing capability to deteriorate |
| 1 | Improve cyber security capability as documented |

### 6.1.1 Option 0: Do Nothing

The option of **'Do Nothing'** assesses the scenario where this initiative is not approved.

**Table 7 Option 0 – Scenario Assessment**

| Criteria | Advantages | Disadvantages |
|---|---|---|
| **1. Solution effectiveness** | | Unable to meet growth, availability, audit and risk requirements. |
| **2. Cost** | Reduced CAPEX | Increased OPEX |
| **3. Business impact** | | Increased frequency and duration of service outages, safety incidents and data breaches with subsequent operational and reputation costs. |

| | | |
|---|---|---|
| | | Compliance breaches relating to state and federal legislative and/or regulatory requirements. |
| **4. Business strategic alignment** | | Not aligned. Security is a cornerstone of building trust with our customers and shareholders. It is a must to ensure reliable operation of our network. |
| **5. IT strategic alignment** | | Not aligned with the principles of maintaining fit for purpose systems in an integrated and efficient manner. |
| **6. Project complexity** | NA | NA |
| **7. Risk profile** | | Increased risks across all areas.<br>See Appendix B - Risk Comparison. |
| **8. Compliance** | NA | Failure to comply with applicable market regulator and other state / federal requirements. |
| **9. Time** | NA | NA |

### 6.1.2 Option 1: Maintain and extend security components

The option of '**Maintain and extend security components**' is the preferred option and its scenario assessment can be seen below. Further details are available on section 6.8 titled "Preferred option".

**Table 8 Option 1 – Scenario Assessment**

| Criteria | Advantages | Disadvantages |
|---|---|---|
| **1. Solution effectiveness** | Able to meet growth, availability and audit requirements. | |
| **2. Cost** | | Increase in CAPEX |
| **3. Business impact** | Reduced frequency, duration and scope of service outages and breaches. | |
| **4. Business strategic alignment** | This option will support the fulfilment of the business and performances objectives detailed in sections 3.1 and 3.2. | |
| **5. IT strategic alignment** | This option will provide TasNetworks with the capability to deliver an adequate security capability across the business. It will also:<br>Be designed to suit TasNetworks work practices and compliance obligations.<br>Be maintainable and supported.<br>Align with current IT infrastructure.<br>Align with other IT road map initiatives. | |
| **6. Project complexity** | | Medium |
| **7. Risk profile** | See Appendix B - Risk Comparison. | See Appendix B - Risk Comparison. |
| **8. Compliance** | Maintains and improves compliance with applicable market operator and state/federal requirements. | |
| **9. Time** | | |

## 6.2 Option estimates

Tables 10 and 11 show the cost estimates for options 1 and 2. Option 0 'Do Nothing' has no capital expenditure.

**Table 9 Option 1 – Cost Estimates**

| Estimate (in nominal dollars) | | | | | |
|---|---|---|---|---|---|
| **Option 1 expenditure profile** | **19/20** | **20/21** | **21/22** | **22/23** | **23/24** |
| Capex | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Opex | | | | | |

**Table 10 Option 0 – Cost Estimates**

| Estimate (in nominal dollars) | | | | | |
|---|---|---|---|---|---|
| **Option 0 expenditure profile** | **19/20** | **20/21** | **21/22** | **22/23** | **23/24** |
| Capex | | | | | |
| Opex | | | | | |

## 6.3 Economic analysis

An economic analysis has been undertaken to compare the options considered. The economic analysis was conducted on the options to address detailed project outcomes. Options were evaluated against Option 0. Details of the NPV analysis are included in Appendix A.

The table below details the preferred option in respect to NPV results.

**Table 13 NPV Summary Results**

| Option No. | Option description | NPV | Reason got selection/rejection |
|---|---|---|---|
| **0** | Do nothing, allowing existing capability to deteriorate | [redacted] | **No business benefit. Leaves significant risk and almost certain operational impact.** |
| **1** | Improve cyber security capability and maturity | [redacted] | **Provides business benefits and mitigates risks in current environment.** |

### 6.3.1 Sensitivity analysis

N/A

## 6.4 Risk Matrix summary of drivers

This matrix provides a comparison of each option's impact against the company risks identified in section 3.3 "Risk objectives". Appendix B contains supporting details of the risk assessment outcomes as summarised in table 13.

(Risk review to be cognisant with risk approach and risk management process outlined in TasNetworks' risk management framework document[3].)

**Table 11 Risk Matrix summary**

| Key Risk | Option 1 | Option 2 |
|---|---|---|
| Failure to address key business cyber security risk consequences in TasNetworks Risk Register | HIGH | MEDIUM |
| Targeted attack resulting in a compromise of the power network | HIGH | MEDIUM |
| Breach of market operator compliance requirements | HIGH | LOW |
| Disclosure of private and/or confidential information | HIGH | LOW |

## 6.5 Quantitative risk analysis

N/A

## 6.6 Benchmarking

N/A

## 6.7 Expert Findings

N/A

## 6.8 Preferred option

The preferred option is to continue upgrading, extending and aligning the cyber security and supporting systems. Primarily this will take the form of periodic upgrades and building our capability, increasing efficiencies through automation and analysis. This insures a vendor supported environment aligning with both the IT and Cyber Security strategies and decreases financial, compliance and network risk by reducing system interruptions, improving visibility and maintaining or improving our security stance. This aligns with the very low appetite the business has to security risk.

### 6.8.1 Scope

The scope of the preferred option includes:

- Improvement of cyber security capability through:
  - Increased maturity of policies and processes against the AESCSF framework
  - Increased implementation of Australian Securities Directorate mitigation strategies.

[3] *Zone Ref. R0000209885*

- Maintenance of current cyber security operational controls through:
    - Maintenance, upgrade, extension and replacement of security hardware
    - Maintenance, upgrade, extension and replacement of supporting software and management components dedicated to the security of the network core and perimeter
    - Maintenance, upgrade, extension and replacement of supporting software and management components dedicated to the security of the environment and end points. End points include servers, desktop devices and mobile devices.
    - External and internal security and auditing tests and resulting action items
    - Enforcing and auditing access controls at the software, user and network levels
    - Enforcing and auditing digital rights controls on high value digital assets.

### 6.8.2 High Level Implementation Activities

The high level implementation activities of this initiative are:

- Review on a regular interval capacity and performance requirements and trends for the products in scope of this initiative
- Procure capacity and introduce capability based on the above analysis
- Plan and action project initiatives in line with recommendations and business needs.

# 7. Investment timing

This investment is part of a rolling upgrade and migration process. Upgrades are staggered over the period with capability incrementally rolled out.

# 8. Regulatory test

N/A

# 9. Expected outcomes and benefits

The outcomes and benefits are considered from a TasNetworks perspective and from an external stakeholder perspective, in this case the customer and retailer. Details of these benefits can be seen in the table below.

Essentially the benefits will be a lessening of risk outlined in the tables above but more specifically the preferred option will:

- Maintain or improve incidence response times leading to critical and ancillary systems being more available to both internal and external customers
- Harden our security stance increasing the time between incidents and decreasing the scope of these incidents
- Auditing and other records will be more complete and timely

- Data generated from our internal systems will be analysed in an increasingly automated fashion from a security related standpoint.

**Table 12 Summary of Expected Benefits**

| | |
|---|---|
| **TasNetworks' perspective** | **Tangible benefits**<br>The potential benefits of the preferred option are consideration reduction of costs incurred from a potential security incident.<br>**Benefit Description** / **Benefit**<br>[redacted]<br>**Intangible benefits**<br>This project will provide the following benefits:<br>▪ Maintain the safety of the electricity supply network<br>▪ Maintain integrity of systems and data.<br>▪ Maintain confidentiality of data.<br>▪ Maintain high availability of systems.<br>▪ Maintain sufficient performance of systems. |
| **Customer's perspective** | ▪ Maintain high availability of systems.<br>▪ Maintain integrity of systems and data.<br>▪ Maintain sufficient performance of systems.<br>▪ Maintain customer trust. |

# 10. Assumptions

The table below shows the assumptions used for this IES.

**Table 13 Assumptions**

| ID | Assumption Description |
|---|---|
| ITA-081 | No major stepwise increase in requirement from initiatives outside of Infrastructure. |
| ITA-082 | Equivalent capacity between similarly priced equipment 5 years apart is 3x (based on existing compute infrastructure compared to the replacement equipment quoted in the detailed costs) |
| ITA-086 | This analysis breaks down after 2 years of extension as it is no longer possible to acquire hardware maintenance contracts on equipment of this age. A more practically relevant analysis would require that replacement is unavoidable at year +6 or +7 and those capital costs should be deferred those years rather than eliminated. |
| ITA-089 | No significant change in employee numbers. |
| ITA-079 | No significant move to externally hosted services (cloud). |
| ITA-080 | AI based systems will still be considered immature and not widely adopted. |
| ITA-135 | As security systems age increasing amount of manual work by IT operations must be performed. 0.5 days/week |
| ITA-136 | As security systems age they will be less agile which will result in project and initiative delays as service requests are processed. 2 days a month for a team of 20. |

| | |
|---|---|
| ITA-137 | Scope and frequency of security incidents increase as systems are outpaced by the threat landscape. Minor incidents result in operation impacts of 500k (industry standard). This includes investigation and remediation. |
| ITA-147 | Frequency and impact of security breaches and incidents has been averaged over the determination period. |
| ITA-148 | Compliance with AESCSF practices will be recommended or mandated by the market operator during the determination period. |
| ITA-149 | Implementation of ASD mitigation strategies will be recommended or mandated by the market operator during the determination period. |

# 11. Recommendation

It is recommended that the preferred option is approved and progressed as it best satisfies the customer and business needs.

# Appendix A – NPV analysis

| | Option 0 | Option 1 |
|---|---|---|
| [redacted] | | |

# Appendix B - Risk Comparison

The project options each have a different impact on the future asset risk. The table below provides a qualitative summary of the risk considerations cognisant with risk approach and risk management process outlined in TasNetworks' risk management framework document[4]] and complement the risks identified in section 3.3 "Risk objectives".

| Key Risk | Consequence | Likelihood | Rating | How does this option mitigate current situation risk? | Consequence | Likelihood | Rating | How does this option mitigate current situation risk? |
|---|---|---|---|---|---|---|---|---|
| Failure to address key business cyber security risk consequences in TasNetworks Risk Register | SEVERE | POSSIBLE | HIGH | No mitigation | MODERATE | UNLIKELY | MEDIUM | • Global reduction in risk likelihood through program execution<br>• Global reduction to risk impact through program execution<br>• Specific initiatives to address key risks |
| Targeted attack resulting in a compromise of the power network | SEVERE | UNLIKELY | HIGH | No mitigation | HIGH | RARE | MEDIUM | • Maintains existing avoidance and mitigation measures<br>• Improvements to avoidance and mitigation measures through program execution |
| Breach of market operator compliance requirements | MODERATE | ALMOST CERTAIN | HIGH | No mitigation | MINOR | RARE | LOW | • Improved compliance with both ASD and AESCSF framework maturity levels |
| Disclosure of private and/or confidential information | MODERATE | LIKELY | HIGH | No mitigation | MINOR | UNLIKELY | LOW | • Maintains existing avoidance and mitigation measures<br>• Improvements to avoidance and mitigation measures through program execution |

[4] ZoNe ref. R0000238142.