Enhanced Supply Chain, Personnel and Risk Management Plan Business Case

2023-28 Revised Revenue Proposal

Approvals

Author	Matt Riley	**Head of Business Resilience**
Endorsed	Peter Gay	Head of Security Strategy
	Andrew Webster	Chief Security Officer
Approved	Robert McKimm	Chief Risk Officer
Date submitted for approval	11 November 2022	

Change history

Revision	Date	Amendment
0	25 Oct 2022	Initial issue
1	11 Nov 2022	Final amendments

Summary

Transgrid now has a regulatory obligation to meet the requirements of the Security of Critical Infrastructure Act, 2018 (SOCI) and the subsequent legislation amendments. This legislation has introduced all-hazards positive security obligations for four key pillars:

- Cyber and information security hazards
- Personnel hazards
- Supply Chain hazards
- Physical and natural hazards

These pillars are held together by a critical infrastructure risk management plan that aims to minimise and mitigate the effects of a hazard being realised.

Today's threats are a result of hybrid attacks targeting physical and cyber assets, supply chain and key personnel. The increasingly interconnected cyber-physical Operational Technology (OT) systems means the attack surface has expanded resulting in software and other types of supply chain attacks that were largely irrelevant to OT, are now highly relevant.

Through comprehensive personnel vetting and other processes associated with critical roles and employees, organisations can assess potential risks presented by personnel. Depending on position type and position risk, Transgrid will determine an individual's suitability to work in a specific position, have access to sensitive information and be in a position to manage critical infrastructure.

In addition, Transgrid is required to adopt and maintain an all-hazards critical infrastructure risk management plan. Organisations with converged cyber, supply chain, personnel and physical risk management and security functions are more resilient and better prepared to identity, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified continuity and resilience related policies across business units.

This business case addresses the resources necessary to support the improvement in controls associated with personnel and supply chain and the overall risk management plan to support the pillars. The delivery of this business case enables Transgrid to be able to meet our regulatory reporting obligations and whilst these are legislated obligations, the rules show a clear way to be better at security in these areas. Achieving that level will improve the overall resilience of Transgrid.

Including protective security into a broader and more mature approach will improve the overall resilience of Transgrid. At the same time, improvements are being made to the emergency/crisis management and business continuity processes, to minimise impact and return to as close to BAU as possible following a major interruption.

The next phase following process improvements to protective security and resilience is to automate. Sourcing and implementing a 'best for Transgrid' automation platform, this will promote our innovation roadmap reduce costs and provide a 'force multiplier' to the strong foundational processes built to support Transgrid's strategy.

Personnel hazards

The SLACIP Bill requires Transgrid to establish and maintain processes and systems for:

- identifying critical workers
- assessing on an on-going basis the suitability of a critical worker to have access to the critical components of a critical asset
- minimising or eliminating material risks that negligent employees and malicious insider man cause to the functioning of a critical asset
- minimising or eliminating material risks arising from the off-boarding process for outgoing employees and contractors

This is how we identify our critical positions and/or people and ensure their suitability is appropriately managed, including assessing and managing their ongoing suitability through security and human resource arrangements. This includes a program, commensurate with the risk environment, of vetting critical people, to mitigate risks from potentially negligent people and malicious insiders who could cause damage to the functioning of our critical infrastructure. The end-to-end program also covers how we manage risks in the off-boarding process for outgoing personnel.

This program is also a key element in the development of Fraud & Corruption (F&C) Management. As Transgrid grows and invests significantly in transitioning to a clean energy future, a robust F&C Management program is essential.

As per Australian Cyber Security Centre (ACSC) personnel security guidelines, the following controls address personnel hazard risk:

- A background check under the AusCheck scheme for assessing the suitability of critical workers, once identified, to have access to the critical components of an asset will be performed.
- Enhanced cyber security awareness training tailored to the needs of specific teams and business units. For example, personnel with responsibilities beyond that of a normal user will require tailored privileged user training.
- Detecting, managing and reporting suspicious changes to banking details or payment requests. Business email compromise, a form of financial fraud, is when an adversary attempts to scam an organisation out of money or assets with the assistance of a compromised email account. To mitigate risk of business email compromise, the following is required:
  - Enhanced monitoring of changes to banking, payment details including changes to baseline payment activity
  - Personnel education for warning signs such as suspicious email addresses not matching an organisation's name
  - Advising personnel of what suspicious contact via online services is and how to report it
  - Advising personnel to take special care not to post work information to online services unless authorised to do so.
- Minimise risk of malicious actors developing a detailed understanding of critical worker lifestyle and interests that could be used to build trust in order to elicit sensitive or restricted information and/or

influence them to undertake specific actions such as opening a malicious email or visiting a malicious website.

- Sending and receiving files via online services, if not blocked outright, personnel need to be advised not to send or receive files via unauthorised collaboration tools.
- Documenting system and data access requirements to assist with determining if personnel have the appropriate authorisation, security clearance, briefings and need-to-know access. Types of users for which access requirements will be documented include unprivileged users, privileged users, foreign nationals, and contractors

Personnel hazards resource requirements and investment

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[1]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[1] Not including CPI increases

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[1]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[1]
Total		**$651,000**	**$370,000**

Supply chain hazards

A supply chain is a complex series of interactions across the lifecycle of all products and services used by Transgrid. Every time Transgrid interacts with a supplier, manufacturer, distributor, or retailer there is an inherent risk. As such, these businesses can potentially compromise Transgrid's systems and data.

A number of high-profile supply chain cyber security related breaches have occurred with material impacts to organisations as a result failures in the supplier ecosystem. A significant global supply chain cyber-attack occurred in 2020 that exploited the software update process and vulnerabilities in Microsoft, SolarWinds and VMware products. The attack went undetected for months and is considered to be among the worst cyber-espionage incidents ever suffered by the United States.

Effective cyber supply chain risk management ensures, as much as possible, the secure supply of products and services for systems throughout their lifetime. This includes their design, manufacture, delivery, maintenance, decommissioning and disposal. As such, cyber supply chain risk management forms a significant component of any organisation's overall cyber security strategy.

Supply chains have also been under strain due to high demand, constricted logistics capacity, pandemic related lockdowns which have amplified labour shortages, raw material and equipment shortages. Complex risks posed by suppliers, products, pricing, regulations, and geo-political events can be modelled, quantified, and monitored via the use of dedicated supply chain resilience services.

To build greater supply chain resilience, Transgrid needs to undertake detailed analysis of its supply chain risk which involves understanding:

- Nationality of suppliers, manufacturers and other critical parts of the supply chain across the lifecycle of critical assets (design, manufacture, delivery, maintenance, decommissioning and disposal) and other factors that would classify a vendor as high risk
- Any failure or lowered capacity of assets and entities in Transgrid's supply chain
- To what extent a business might be controlled, influenced and/or interfered with by a foreign entity
- Risks associated with poor security practices such as employee background checks, cyber security practices and protection of their own supply chain
- Threats to people, assets, equipment, products, services distribution, and intellectual property within the supply chain
- Use of genuine products and parts
- Contractual terms and conditions that explicitly address supply chain risk, provide for requirements such as transparency of assessments, testing of security practices, vulnerability disclosure
- Access and privilege risks including if products and services minimise the requirement for unnecessary privileges

- Risk of stolen or abused credentials to exfiltrate data and/or compromise critical asset control
- Location of support and data storage to ensure compliance with license requirements
- Sourcing from countries and/or organisations subject to sanctions, export restrictions, sovereign trade policies
- Impact of regulatory and political change

To address these risks the following is required

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[2]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[2] Not including CPI increases

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[2]
Total		**$520,000**	**$440,000**

Critical Infrastructure Risk Management Plan

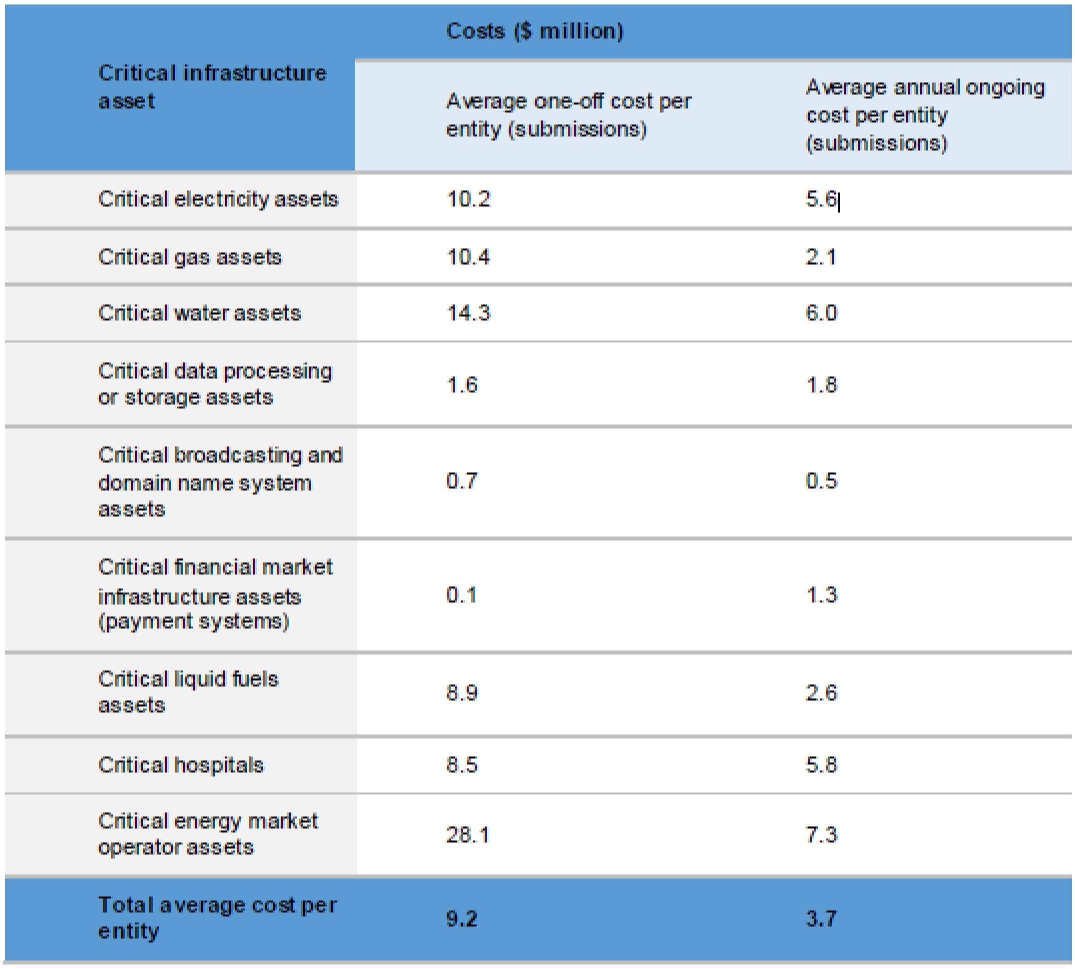
To ensure cyber, physical and natural hazard, personnel and supply chain security and hazard risks and their respective controls enhancement programs are managed in a coordinated and holistic manner, Transgrid needs to enhance its critical infrastructure risk management processes and capabilities.

Analysis completed by KPMG for the electricity and gas sectors, shows a severe incident on the electricity sector could cost as much as $1.280 billion to the economy in direct and indirect costs. Consumers could also face flow-on price increases as a result of an incident. A moderate incident to the electricity sector is estimated to cost approximately $850 million - more than triple the estimated $225.6 million annual ongoing cost of the mitigating measures.

In addition to the costs to the economy, a disruption to these services would have a significant impact on Australia's social stability, defence, national security capabilities and could have an effect on the ability of the Australian government to govern effectively. The risk management program reforms under the SLACIP Bill have a strong cost prevention element, ensuring that the net benefits to the economy as a whole outweigh the initial costs on industry.

In contrast, analysis of the average expected costs for responsible entities to implement, and maintain, the risk management program rules is currently an average one-off cost of $9.2 million followed by an average ongoing cost of $3.7 million per annum (p.a.), from the data provided so far. Although these figures are, in a relative sense, quite low, they do provide an insight into the current state of risk management amongst Australia's critical infrastructure entities and the need for further action to be taken.

Source: Department of Home Affairs submission into the Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 - Parliamentary Joint Committee on Intelligence and Security February 2022



Critical infrastructure asset	Costs ($ million)	
	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	10.2	5.6
Critical gas assets	10.4	2.1
Critical water assets	14.3	6.0
Critical data processing or storage assets	1.6	1.8
Critical broadcasting and domain name system assets	0.7	0.5
Critical financial market infrastructure assets (payment systems)	0.1	1.3
Critical liquid fuels assets	8.9	2.6
Critical hospitals	8.5	5.8
Critical energy market operator assets	28.1	7.3
Total average cost per entity	**9.2**	**3.7**

Source: Draft RIS for draft RMP rules dated February 2022.

Under the SOCI legislation, Transgrid needs to develop a Risk Management Plan (RMP) that takes an “all hazards” approach to safeguarding business assets and our people. The following high-level approach for meeting RMP legislation rule requirements:

- Establish a SOCI governance structure and committee – include members from respective business functions
- Obtain legal advice to provide a deep understanding and interpretation of legislative requirements, the applicability of the requirements to Trangrid, and the adoption of a position in relation to the legislative requirements supported by relevant law’s and statutes
- Define and formally document an enterprise RMP
- Identity Critical Infrastructure (CI) assets
- Populate CI asset details with metadata associated with location, dependencies, upsteam and downstream relationships, availability, cyber, supply chain and personnel security related risks
- Assess CI asset risks from an “all hazards” perspective commencing with the four hazard domains defined in the RMP rules
- Prioritise CI asset risks and align to remediation program scope and timing

- Security Program Governance Committee to endorse CI risk mitigation
- Risk mitigation activities commence
- Evidence of risk mitigation via quantitative and qualitative metrics and measures used for internal and external stakeholder reporting

TransGrid will provide an annual risk management plan report including:

- Whether or not the program was up to date during the financial year
- If a hazard had a significant relevant impact on one or more critical assets, including a statement that:
    - Identifies the hazard
    - Evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on relevant critical assets
    - Outlines any variations made to the program as a result of the hazard occurring

Organisations with converged cyber, supply chain, personnel and physical security risk management are more resilient and better prepared to identity, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified continuity and resilience related policies across business units.

An integrated risk management strategy reflects in-depth understanding of the cascading impacts to interconnected cyber-physical infrastructure and relationships to supply chain and personnel hazards. The following benefits are derived from a converged risk management program:

- Holistic view of risk posture available to senior management
- Duplication reduction
- Greater alignment to enterprise strategies
- Information sharing and utilisation of best practices
- Risk reduction, controls implementation program easier to manage via a single set of shared practices and objectives

The enterprise risk management program acts as a line 2 governance function over lower level risk management functions that reside with personnel, supply chain, physical and natural hazard and cyber-security hazard line 1 teams.

To ensure Transgrid can efficiently plan for, respond to and improve the management of critical events and exercises, a dedicated Software as a Service (SaaS) solution is required. Key benefits of adopting a dedicated platform for crisis management are:

- Automated workflows and checklists that lets teams focus on resolving issues, not completing admin work
- A single source of truth for essential data including response plans, procedures, and situation reports
- Adaptable to processes in different business units
- Can be used on mobile devices, laptops from any authorised location

This business case includes essential initiatives required to enhance Transgrid's existing risk management program are:

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[3]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[3] Not including CPI increases

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[3]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
Total		**$945,000**	**$900,000**

Financial Breakdown

Total incremental cost for the resources necessary to support the improvement in controls associated with personnel and supply chain and the overall risk management plan to support the pillars

$	#	FY24	FY25	FY26	FY27	FY28
Personnel	New	651,000	370,000	370,000	370,000	370,000
Supply Chain	New	520,000	440,000	440,000	440,000	440,000
Risk Management Program	New	945,000	900,000	900,000	900,000	900,000
TOTAL		**2,116,000**	**1,710,000**	**1,710,000**	**1,710,000**	**1,710,000**

Response to the AER's Draft Decision – Physical & natural hazards security

The costs for physical and natural hazards security were included in our initial step change. Our initial step change included physical security external assurance activities of $1.0 million, which the AER's Draft Decision found were not justified. We accept that additional information is required to justify these costs, which is included below.

The following costs do not relate to our additional costs for personnel, supply chain and the risk management program. The following information and costs provide additional justification for the physical security assurance activities included in our initial revenue proposal step change.

We manage physical and natural hazards at the sites we assess as critical by minimising and mitigating risks and impacts of unauthorised access, interference and/or control as well as the relevant impact of natural hazards.

Our assurance activities will develop risk-based Security Management Plans detailing how we;

- Respond to unauthorised access;
- Control authorised access, including restricting access to only people with the appropriate approval who have an operational need to access;
- Conduct tests and provide assurance that active security measures are effective and appropriate to detect, delay and deter breaches; and practice how we will respond and recover from breaches of security; and
- Minimise, mitigate and recover from the impacts of natural hazards and disasters, including but not limited to bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis, health hazards such as pandemics.

The resource requirements for these assurance activities are:

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[4]
[redacted]	[redacted]	[redacted]	[redacted]

[4] Not including CPI increases

Requirement	Quantity	Opex FY24	Opex FY25+ per annum[4]
[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
Total		$365,000	$365,000

These forecast costs are slightly higher than our initial step change for physical security assurance activities, however we maintain our initial step change forecast for physical security assurance in our Revised Revenue Proposal.