Options Evaluation Report (OER)

Cyber Security

Approvals

Author	Braam Broodryk	Security Strategy Manager
Reviewed	Delan Naidu	IT Domain Manager (Technology)
	Sophong Tran	IT Performance and Governance Associate
Approved	Russell Morris	CIO
Date submitted for approval	15 November 2021	

Change history

Revision	Date	Amendment
Draft v1	04 Apr 21	New revised, short form draft OER
0.2	10 Sept 21	Updated version for iteration 6 submission
1.0	15 Nov 21	Updated version for November submission

Executive summary

This OER sets out how we propose to meet the increased security and resilience requirements in the current draft of the Critical Infrastructure Bill 2021 (CI Bill) for Systems of National Significance.

As a critical infrastructure provider, we need to prepare to comply with the enhanced regulatory framework proposed by the CI Bill, which builds on the Australian Energy Sector Cyber Security Framework (AESCSF).

We have already invested in security controls and capabilities to manage the changing cyber threat landscape and is currently self-assessed at a Maturity Indicator Level rating of [redacted] under the AESCSF.

However, to comply with the proposed CI Bill, we expect to have to gain and maintain an AESCSF Security Profile (SP) rating of 3 (or its equivalent), requiring achieving MIL-3 ratings across all relevant domains. To reach this mandated increase in security, we will need to refresh or improve our current controls and implement new controls.

The CI Bill is expected to be passed into law in November/December 2021 at the earliest. The costings in this OER represent are based on the current proposed bill. We will refine our final submission to align with the final bill once it has been passed.

In addition to the CI Bill, Transgrid will also need to comply with other new legislative requirements, including:

> Energy Legislation Amendment Bill 2021 (NSW)

> Ransomware Payments Bill 2021

Even though the additional legislative requirements exist, the initiatives set out in this OER should enable Transgrid to comply with their associated obligations.

The proposed option in this OER will:

> Allow us to comply with the legislative requirements set out in the CI Bill, including meeting the sector-specific maturity rating of AESCSF SP-3 or its equivalent as well as other legislative requirements recently introduced or in the process of being introduced;

> Be achievable within the timeframe required by the bill;

> Leverage previous investments made in reaching [redacted] and maximise re-use where possible;

> [redacted]; and

> Remediate capability gaps following a least cost approach to meeting the CI Bill's requirements.

We have considered alternative, lower cost options for this OER. But none would fully comply with the requirements set out in the current draft of the CI Bill. As such, these alternative options have been ruled out and not considered in this OER.

Below is a summary of the only option that will allow us to meet our regulatory obligations.

Option	Description	Direct Capital cost ($M)	Network & Corporate overheads ($M)	Total Capital cost ($M)	Net Present Value (NPV) ($M)	Rank
Full compliance with Critical Infrastructure Bill requirements.	Enhancing our cyber security capabilities to meet all the requirements of the proposed Critical Infrastructure Bill, including meeting sector-specific rules e.g. AESCSF SP-3 maturity or equivalent.	[redacted]	[redacted]	$14.710	N/A	1

The proposed capital expenditure for this OER is summarised below.

IT Capex $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Non-Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
TOTAL	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	$14.710M

[redacted]

The numbers in this OER represent the total cost of ownership for an asset consistent with past submissions.
There has been a change in accounting practices associated with IFRS[1] that has come in place.
The proposed capital expenditure for preferred option in this OER shown with IFRS impact is below

IT Capex IFRS $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Non-Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
TOTAL	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	$14.176M

The change in IFRS capex is the result of software subscriptions proposed as part of the preferred solution.

[1] International Financial Reporting Standards Foundation (IFRS Foundation) ruling means that in the 2023-28 period we will expense costs for configuration or customisation in cloud computing arrangements, whereas in the 2018-23 regulatory period these costs were treated as capex.

1. Background

The Australian Government is committed to protecting the essential services that all Australians rely on. The Government considers the threat of a cyber-attack on Australia's critical infrastructure to be "immediate", "realistic" and "credible", with the potential to take down the nation's electricity network at immense impost to society and economy.

The Department of Home Affairs is progressing the need for tighter cyber security in national assets through the Security Legislation Amendment (Critical Infrastructure) Bill 2021 (Cth) (CI Bill) and Systems of National Significance reform. The reform embeds preparation, prevention and mitigation activities into the business-as-usual operating of critical Australian assets, including those operated and maintained by us.

The Situational Awareness program funded in the current regulatory period has given us a strong set of foundational security controls and processes. This program successfully implemented new SIEM and CASB solutions to provide more cost effective solutions to enable visibility of security and operational related events. During the current regulatory period, the following foundational controls were implemented:

- Enterprise Log Management and User Behaviour Analytics foundations
- Insider threat detection
- Endpoint detection and response
- ISO27001 certification
- Data Leakage Prevention
- Cloud Access Security Broker (CASB)
- USB lockdown
- Field staff tools PC
- Secure remote access protocol (SCADA)
- Identity Management, including Privileged Identity Management
- Utilising a Managed Security Service Provider (MSSP) for Level / Tier 1 Security Support, paving the path to move to 24 x 7 monitoring capability

[redacted]

1.1 Why is this important?

Our current Security Profile rating will not meet the requirements of the new legislation, which is expected to require AESCSF SP-3 maturity or its equivalent. Raising our security level to SP-3 is essential for our future:

- **Security**: Failure to appropriately address security risks and vulnerabilities exposes us to security weaknesses, which would result in major service disruptions as well as financial and reputational penalties.

- **Regulatory compliance**: Critical infrastructure underpins the delivery of goods and services that are essential to the Australian way of life, our nation's wealth and prosperity, and national security. Complying with the CI Bill will allow us to enhance our operations, protect our customers and partners and appropriately manage security risks. While sector-specific rules are still to be finalised, there is a high degree of confidence that the rules will require critical infrastructure energy utilities to adopt AESCSF with a Security Profile of 3 (or equivalent as the AESCSF framework is currently being updated).

1.2 The Critical Infrastructure Bill

1.2.1 Background of the bill

In response to cyber security and critical infrastructure concerns, the Federal Government passed the Security of Critical Infrastructure Act 2018 (CI Act), which introduced obligations in the electricity, gas, water and ports sectors to ensure the physical and electronic security of Australia's critical infrastructure.

The Government is presently tabling a proposed Bill amendment to introduce an enhanced regulatory framework that increases the security and resilience requirements of Australia's critical infrastructure. This builds on work completed by AEMO.

1.2.2 Requirements under the CI Bill

When enacted, the CI Bill 2021 will require us, as the operator of critical transmission infrastructure, to:

- Meet sector-specific requirements for the electricity sector and telecommunications sector, which is expected to require achieving the equivalent of MIL-3 across all domains to reach and sustain SP-3 or its equivalent
- Implement an all-hazards critical infrastructure risk management program addressing natural and human induced risks
- Report cyber security incidents to the Australian Signals Directorate
- Continue reporting ownership and operational information (including outsourcing and off-shoring) in the Department of Home Affairs' Register of Critical Infrastructure Assets
- Undertake prescribed cybersecurity activities anticipated for Systems of National Significance, including:
- Incident response plans;
- Cyber security exercises;
- Vulnerability assessments; and
- Access to system information.

TransGrids compliance timings under the CI Bill 2021

	Compliance requirements	[redacted]
Cyber Security	Meet SP-1 of the AESCSF Framework	[redacted]
	Meet SP-2 of the AESCSF Framework	[redacted]
	Meet requirements that will be based on the new AESCSF Framework currently being drafted, but likely akin to the SP-3 requirements in the existing framework.	[redacted]
Personnel Security	Develop a process for determining critical employees, contractors and sub-contractors	[redacted]
	Ensure our risk management program includes details of processes used to determine critical employees	[redacted]
	Ensure our risk management program includes details of how background checking (both for new and ongoing employees) are conducted, having regard of AS 4811-2006, or the most recent version of this standard, or an equivalent standard	[redacted]
	Ensure critical employees, engaged 12 or more months after the commencement of the rule, undertake and pass a background check under the AusCheck scheme	[redacted]
	Ensure our risk management program includes details of how we: > Assess and manage the ongoing suitability of its self-assessed critical employees, contractors and subcontractors > Manage the risk of insider threats to the asset, including but not limited to negligent employees and malicious insiders > Manage risks arising from the off boarding process for staff, contractors and subcontractors > Manage risks arising from existing employees who fail to maintain suitability.	[redacted]
Supply Chain Security	Ensure our risk management program includes details of how we comply with the requirements of: > ISO 28001:2007 Security management systems for the supply chain Best practices for implementing supply chain security, assessments and plans Requirements and guidance or an equivalent standard	[redacted]

	> ISO 28000:2007 Specification for security management systems for the supply chain or an equivalent standard > ISO 22301:2019 Security and resilience Business continuity management systems Requirements or an equivalent standard.	
	Demonstrate how our risk management program, as far as is reasonably practical, minimises and mitigates relevant impacts to the asset arising from the supply chain, including but not limited to: > Unauthorised access, interference or exploitation > Privileged access > Disruption and sanctions > Threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains	[redacted]
Physical Security	Ensure our risk management program sets out how we: > Detect and deter unauthorised persons accessing secure areas, and respond to incidents where unauthorised access occurs > Restrict, control and monitor access by unauthorised persons > Control authorised access, including restricting access to only those persons with the appropriate approval who have an operational need to access.	[redacted]
	Demonstrate in our risk management program how we conduct tests, as appropriate, to ensure active security measures are effective and appropriate to detect, deter, respond to and recover from breaches of security at self-assessed critical sites. These tests may be conducted in conjunction with other safety, security or emergency management exercises or procedures.	[redacted]
	Ensure our risk management program sets out how we have regard to ENA Doc 015 2006 “National guidelines for prevention of unauthorised access to electricity infrastructure”.	[redacted]

To comply with these security obligations in Information Technology (IT), Operational Technology (OT) and protecting physical infrastructure, we need to increase our operating and capital expenditure.

[redacted]

[redacted]

[redacted]

[redacted]		
[redacted]		

In addition to using the AESCSF as a mandated framework, we have also adopted the ISO/IEC 27001 framework to manage security related activities and risks as part of an Information Security Management System (ISMS). A risk-based approach was used to determine the appropriate treatment, considering the potential business impact of different incidents (e.g. data loss, ransomware attack).

2. Related ICT Programs

This table describes why this Cyber Security OER is important to the other OERs.

ICT Programs/OERs	Importance to other OERs*	Relationship commentary
Application Maintenance / Bespoke Applications	High – compliance	Includes applications covered by the regulatory security obligations supported by this OER.
Customer Safety & Support	High – compliance	Covers personally identifiable information that must be kept secure and in compliance with the Privacy Act 1988 and protected to maintain compliance with our Operating Licence.
Data & Decisioning	High – compliance	Covers the security classification of data used in identity management solutions and drives security control requirements. The design of the data warehouse will be impacted by the recommendations of this OER.
Employee Enablement	High – compliance	Includes operating environment and team collaboration tools covered by the regulatory security obligations supported by this OER.
Infra. & Network	High – compliance	Includes the cyber security equipment and applications recommended in this OER.
Operational Efficiency / Evolution	High – compliance	[redacted]

* KEY
High – the OER is essential from a functional or compliance perspective to another OER
Medium –the OER is required to fully realise the benefits of another OER or would result in a change in scope
Low – the OER is has a low level of dependency to another OER

3. Option summary

3.1 Single Option – Meeting the full requirements of cyber compliance obligations, including expected sector-specific rules of AESCSF SP-3 compliance.

3.1.1 Description

During the 2023-28 regulatory period, we will continue its journey of improving maturity against the Australian Energy Sector Cyber Security Framework (AESCSF), with the intention of meeting the proposed legislative requirement of AESCSF Security Profile (SP) 3 within five years of the CI-Bill becoming effective. All the initiatives proposed in this option are geared to attain this Security Profile.

[redacted]

This option will:

> Allow us to comply with the legislative requirements set out in the bill, including meeting sector-specific maturity rating of AESCSF SP-3 or its equivalent

> Increase the level of automation in our control validation and vulnerability remediation capabilities

> Be achieved within the timeframe required by the bill

[redacted]

3.1.2 Financial summary

The total IT capital expenditure for this option is estimated to be **$14.710M** spread across the five-year regulatory period as shown below:

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Non-Recurrent costs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
TOTAL	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	$14.710M

The costs were based on previous project implementations and vendor quotes. Analysis of existing controls versus future control requirements and a financial analysis and validation of our estimates was performed by [redacted]

[redacted]

In addition, the following benefits have been identified for this option:

3.1.2.1 Quantifiable benefits

N/A.

3.1.2.2 Non-quantifiable benefits

Compliance with the Protecting Critical Infrastructure and Systems of National Significance reform and additional automation would:

- Protect our significant national critical infrastructure
- Support compliance with the Critical Infrastructure Bill legislation and AESCSF requirements
- Support compliance with the Systems of National Significance reform
- Support ongoing compliance with licence obligations
- Align with proposed levels of maturity
- Avoid regulatory breaches and associated noncompliance fines and penalties
- Avoid penalties associated with breach of licence conditions
- Improve speed in identifying and remediating vulnerabilities, protecting the network and customers
- Improve security reporting capability across the business which results in better decision making and a reduction in the time required to generate the reports
- Address the strategic risk related to Protective and Cyber Security
- Improve response times and consistency of approach through greater automation

3.1.2.3 Net Present Value (NPV)

N/A.

3.1.3 Residual Risk

The specific risks and mitigations associated with this option are:

Risk	Mitigation	Residual Risk Level
Are not compliant with the Critical Infrastructure Bill 2021 or System of National Significance reform	This option ensures we meet our compliance and regulatory obligations.	LOW
Exposed to increasingly frequent and severe cyber-attacks	Strategic enhancements in our cyber posture, which comply with the legislation, ensure we mitigate the threat to keep up with the evolving cyber threat landscape.	MEDIUM

Under this scenario, the residual risk associated with this approach is low and is illustrated in the table below:

Table 2. Residual risk (Proposed Option)

	WHS	Reputation	Compliance	Reliability	Finance	People/IR	Environment	Risk
Likelihood	Unlikely	Possible	Unlikely	Unlikely	Unlikely	Possible	Possible	MEDIUM
Consequence	Minor	Moderate	Minor	Moderate	Minor	Minimal	Minimal	
Risk Level	LOW	MEDIUM	LOW	MEDIUM	LOW	LOW	LOW	

3.2 Options considered and not progressed

Option	Reason for not progressing
Do Nothing Option	[redacted]

4. Evaluation

4.1 Commercial Evaluation

The commercial evaluation of the options is set out in the table below.

Table n – Commercial evaluation

Option	Description	Capex ($M)	Benefits ($m/p.a)	NPV ($M)	Rank
Preferred	Compliant with CI Bill, including sector-specific rules.	$12.395	N/A	N/A	1

(Refer to separate costing models for detailed breakdown of these costs)

The above commercial evaluation is based on a:

> 4.8% discount rate

> 5-year discount period

Due to the timing of costs and the absence of financial benefits, this comparison is not sensitive to changes in the discount rate.

Option	Description	Discount rate at 2.23% NPV $M	Discount rate at 7.37% NPV $M
Preferred	Compliant with CI Bill, including sector-specific rules.	$13.567	$11.360M

4.2 Risk assessment

The risk assessment of the option considered is illustrated in the table below:

	WHS	Reputation	Compliance	Reliability	Finance	People	Environment	Overall Risk Rating
Preferred	LOW	MEDIUM	LOW	MEDIUM	LOW	LOW	LOW	MEDIUM

The recommend option has a Medium Overall Risk Rating because it ensures that we comply with the regulatory standards of the Critical Infrastructure Bill and the Systems of National Security reform.

4.3 Regulatory Investment Test (RIT-T)

No RIT-T analysis is required under current rules.

5. Preferred Option

This report recommends proceeding with the proposed option.

The tables below outline the investment, any potential step change in operating costs and the associated benefits of the preferred option.

5.1 Estimated capital costs

Category	Item	Budget ($M)
Material	[redacted]	[redacted]
Labour	[redacted]	[redacted]
		[redacted]
Direct Capex:		[redacted]
Network and Corporate Overheads		[redacted]
Capex Total:		***$14.701***

5.2 Estimated Opex Step Change

Opex Step Change Year of Change	FY24	FY25	FY26	FY27	FY28	End Of Period
Cumulative Step Change	$3.543M	$3.543M	$3.543M	$3.543M	$3.543M	$17.713M

Note: This does not include the Opex step change associated with Physical Security Assurance Activities which has been included in the combined ICT / OT / Physical Step Change submission.

5.3 Benefits

Benefit	$M/p.a

*Please note benefit calculations will be refined when each of the projects are scoped in detail.

[redacted]

[redacted]