OPTIONS EVALUATION REPORT (OER)

FY24-28 Critical Infrastructure Uplift OT Environment

OER- N2551 revision 0.0

Ellipse project no(s):
TRIM file: [TRIM No]

Project reason: Compliance - Security
Project category: Prescribed - Security/ Compliance

Approvals

Author	Anh Diep	Digital Infrastructure Asset Engineer
Endorsed	Debashis Dutta	Asset Analytics & Insights Manager
	Adam Hoare	Digital Infrastructure Asset Manager
Approved	Andrew McAlpine	A/Head of Asset Management
Date submitted for approval	11 November 2021	

Change history

Revision	Date	Amendment
0	11/11/2021	First Issue

Executive summary

The Federal Government has recently introduced draft versions of the Security Legislation Amendment (Critical Infrastructure, CI) Bill 2020[1], of which proposes to extend the scope of the Critical Infrastructure Act 2018 to cover a wider range of sectors, and introduces a number of additional security and risk management requirements that enhance the overall security posture of these sectors. We expect that the Bill will impose new regulatory obligations requiring us to uplift our cyber security capability and infrastructure security. Of note will be positive security obligations supported by sector-specific requirements, which we anticipate will require us to reach the highest level of maturity of the AESCSF framework – SP-3 within 60 months of the Bill requirements coming into effect.

In October 2021 the NSW State Government introduced the Energy Legislation Amendment Bill 2021[2]. It is anticipated this Bill will be legislated by the end of 2021 and will bring forward the AESCSF compliance timeframe requirements of the Federal CI Act amendment by 12 months. This would result in compliance requirements of SP-1 from Q1 2023, SP-2 from Q1 2024 and SP-3 from Q1 2027.

Failure to comply with these anticipated mandates may place TransGrid at risk of breach of legislative requirements as well as incurring financial penalties.

A number of options, achieving varying levels of compliance with the Bill, have been considered to address this need. The assessment of these options appears in Table 1. An NPV is not calculated for this investment as the need is driven by compliance with legislation.

Table 1 - Evaluated options

Option	Description	Direct capital cost ($m)	Overheads ($m)	Total capital cost[3] ($m)	Weighted NPV (PV, $m)	Rank
Option A	Maintaining Current Maturity	0.19	0.03	0.22	N/A	-
Option B	Complying with Proposed Requirements	1.06	0.17	1.23	N/A	-
Option C	Full Compliance with Critical Infrastructure Bill Requirements	3.59	0.59	4.18	N/A	1

The preferred option is Option C as it is the only technically feasible option that enables TransGrid to achieve full compliance with the requirements of the CI Bill.

Associated cyber security uplifts will require an incremental step change in ongoing operating expenditure. Estimated disbursements are shown in Table 2 below and account for ongoing licencing and support costs and FTE allowances.

[1] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

[2] https://www.parliament.nsw.gov.au/bills/Pages/Profiles/energy-legislation-amendment-bill-2021.aspx

[3] Total capital cost is the sum of the direct capital cost and network and corporate overheads. Total capital cost is used in this OER for all analysis.

Table 2 – Incremental opex step requirements

RP2: 2021/22 ($k)	RP2: 2022/23 ($k)	RP3: 2023/24 onward ($k)[4]
118	765	646

[4] Critical Infrastructure Bill Opex Requirement Report (TRIM reference D2021/01486)

1. Need/opportunity

Growing geopolitical tensions between Australia and its trading partners, foreign investment concerns and increasing evidence of country sponsored cyber-attacks on Australian and international utilities have led to increased focus by government and businesses on Cyber and Critical Infrastructure Security obligations. For TransGrid, the loss of terminal stations or transmission lines through third party control or physical interference represents a risk to public safety and the operation of the critical systems that enable the Australian economy to operate.

The Federal Government in 2018 passed legislation, the Security of Critical Infrastructure Act 2018 (CI Act), which introduced obligations on the electricity, gas, water and ports sector to ensure the physical and electronic security of Australia's critical infrastructure. The Government has also recently introduced draft versions of the Security Legislation Amendment (Critical Infrastructure) Bill 2020[5]. The Bill proposes to extend the scope of the CI Act to cover critical infrastructure in a wider range of sectors, and introduces a number of additional security and risk management requirements that enhance the overall security posture of these sectors. The Bill builds on work completed by AEMO, in collaboration with industry and government stakeholders including the Australian Cyber Security Centre, Cyber and Infrastructure Security Centre, and the Cyber Security Industry Working Group, to develop the Australian Energy Sector Cyber Security Framework (AESCSF)[6].

We expect that the Bill will impose new regulatory obligations requiring us to uplift our cyber security capability and infrastructure security. Of note will be positive security obligations supported by sector-specific requirements, which we anticipate will require us to reach the highest level of maturity of the AESCSF framework – SP-3 within 60 months of the Bill requirements coming into effect. Indicative this will likely be December 2022, and therefore the following compliance timeframes would apply:

- Within 12 months of rule commencement comply with requirements to meet SP-1 of the AESCSF Framework, or from Q1 2024.
- Within 24 months of rule commencement comply with requirements to meet SP-2 of the AESCSF Framework, or from Q1 2025.
- Within 60 months of rule commencement, or from Q1 2028, comply with requirements to meet SP-3 of the AESCSF Framework, or equivalent measure.

In October 2021 the NSW State Government introduced the Energy Legislation Amendment Bill 2021[7]. It is anticipated this Bill will be legislated by Q1 2022 and will bring forward the AESCSF compliance timeframe requirements of the Federal Critical Infrastructure Bill 2020, as above, by 12 months. This would result in compliance requirements of SP-1 from Q1 2023, SP-2 from Q1 2024 and SP-3 from Q1 2027.

Current Cyber Security Maturity within the OT Environment

There are two measures for cyber security capability and maturity in the AESCSF:

- Maturity Indicator Level (MIL) – there are four MILs, MIL-0 through MIL-3
- Security Profile (SP) – there are three alternate groupings of SP-1 to SP-3

Although we have not yet obtained an SP maturity rating, we estimate that we meet 99% of SP-1, 87% of SP-2 and 13% of SP-3 requirements. Our evaluation indicates additional investment in capabilities that do not currently exist within the environment is required. In total, 8 of the 12 AESCSF domains will require an uplift to attain SP-2 compliance, with all 12 domains requiring controls or processes implemented to meet the SP-3 (or equivalent) requirement.

[5] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657
[6] https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources
[7] https://www.parliament.nsw.gov.au/bills/Pages/Profiles/energy-legislation-amendment-bill-2021.aspx

AESCSF domains	% SP-2 attained	% SP-3 attained
Risk Management (RM)	100%	17%
Asset, Change and Configuration Management (ACM)	83%	0%
Supply Chain and External Dependencies Management (EDM)	85%	0%
Identity and Access Management (IAM)	67%	0%
Cyber security Program Management (CPM)	100%	0%
Threat and Vulnerability Management (TVM)	100%	11%
Situational Awareness (SA)	75%	0%
Event and Incident Response, Continuity of Operations (IR)	75%	13%
Workforce Management (WM)	78%	8%
Australian Privacy Management (APM)	86%	60%
Information Sharing and Communications (ISC)	100%	20%
Anti-Patterns (AP)	91%	33%
Total compliance	**87%**	**13%**

Failure to achieve the required level of cyber maturity as mandated the Bill may place TransGrid at risk of breach of legislative requirements as well as incurring financial penalties.

2. Related needs/opportunities

> Corporate Security / IT Critical Infrastructure Uplift Security Project

3. Options

3.1 Base case

The Base Case for this need is to maintain our current cyber security posture of AESCSF MIL-2.

This will not meet the proposed CI Bill requirements and is therefore considered not a viable position to maintain.

3.2 Options evaluated

Option A — Maintaining Current Maturity [NOSA N2551, OFS N2551A]

Cyber security maturity will be retained at AESCSF maturity level MIL-2. Marginal improvements and initiatives will be required in order to maintain current capabilities in the face of an expected growing threat landscape. However, this option does not fulfil the new security obligations as set out in the proposed CI Bill.

Refer to Appendix A for the scope of works. It is anticipated that these works will commence in 2023/24 and commissioned in 2024/25.

Option B — Complying with Core Proposed Requirements [NOSA N2551, OFS N2551B]

This option will implement cyber security program initiatives to comply with the new security obligations from the proposed CI Bill. This option will enable TransGrid to comply with the new security obligations (as they are currently understood), with the exception of sector specific rules.

This option builds upon Option A and contains additional initiatives required for complying with core proposed Bill requirements. Uplifts are proposed through initiatives in the following areas:

- Enhanced MSSP / IR
- Enhanced Patch Management

This option will not meet the mandatory AESCSF maturity level of SP-3, or equivalent measure. This option is considered unviable as would result in major non-compliance with the CI-Bill.

Refer to Appendix A for the scope of works. It is anticipated that these works will commence in 2023/24 and commissioned in 2024/25.

Option C — Full Compliance with Critical Infrastructure Bill Requirements [NOSA N2551, OFS N2551C]

This option will implement security uplifts to comply with the new security obligations from the Bill and mature sufficiently to qualify as SP-3 within the AESCSF, or equivalent measure. This option builds upon Option B and contains additional initiatives required for complying with all Bill requirements. Uplifts are proposed through initiatives in the following areas:

- Enhanced MSSP / IR
- Enhanced Patch Management
- Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)
- Enhanced Identity Governance and Assurance (IGA)
- Enhanced Attack Surface Management & Deception Technology
- Enhanced Network and Firewall Assurance.

Refer to Appendix A for the scope of works. It is anticipated that these works will commence in 2023/24 and commissioned in 2025/26.

3.3 Options considered and not progressed

No other options considered.

4. Evaluation

A commercial evaluation has not been carried out as the need is driven by compliance with legislation.

The cost for each option considered is set out in Table 3.

Table 3 - Commercial evaluation

Option	Description	Total Cost ($m)	Ranking
Option A	Maintaining Current Maturity	0.22	-
Option B	Complying with Core Proposed Requirements	1.23	-
Option C	Full Compliance with Critical Infrastructure Bill	4.18	1

	Requirements		

4.1 ALARP evaluation

TransGrid manages and mitigates bushfire and safety risk to ensure they are below risk tolerance levels or 'As Low As Reasonably Practicable' ('ALARP'), in accordance with the regulation obligations and TransGrid's business risk appetite. This need is compliance driven and there is no safety risk reduction associated with the upgrade of the OT systems. Hence, an ALARP evaluation is not applicable in this case.

4.2 Preferred option

The preferred option to meet the identified need by 2027/28 is Option C. Option C is the only technically feasible option identified that enables TransGrid to achieve full compliance with the new security obligations from the Bill. It is also the only option that is likely to cover any further updates to the Bill.

Capital and Operating Expenditure

Cyber security uplifts associated with the preferred option will require an incremental step change in ongoing operating expenditure. Estimated disbursements are shown in Table 4 below and account for ongoing licencing and support costs, as well at FTE allowances required to ensure uplifted environments remain fit for purpose and have adequate resourcing to maintain.

Table 4 – Forecast opex disbursements

RP2: FY22 ($k)	RP2: FY23 ($k)	RP3: FY24 onward ($k)[8]
118	765	646

Regulatory Investment Test

The program and estimate allows for the appropriate Regulatory approvals as required.

5. Recommendation

It is recommended that Option C – Full Compliance with Critical Infrastructure Bill Requirements be scoped in detail. The total project cost is $4.18 million including an amount of $150,000 to progress the project from DG1 to DG2.

[8] Critical Infrastructure Bill Opex Requirement Report (TRIM reference D2021/01486)

Appendix A – Scope of Works

The table below summarises the initiatives that are applicable to each of the options considered.

Table 5 – Scope of Works

OT Environment	Initiative	Name	OT CAPEX Factor	Description	Options Applicable			Cost
					Option A	Option B	Option C	
SSZ	2	Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)	0.2	Initiative transitions to enhanced access control of access-on-demand / zero trust model.			X	$571,131
SSZ	3	Enhanced MSSP / IR	0.2	Initiative allows a managed security service provider to continuously monitor all logs within the managed SIEM rather than during business hours only.	X	X	X	$59,400
SSZ	4	Enhanced Identity Governance and Assurance (IGA)	0.3	Initiative allows automated governance processes around access requests, granting access and reviewing access.			X	$1,126,224
SSZ	5	Enhanced Patch Management	0.5	Initiative enhances patch management capabilities and better enables TransGrid to address vulnerabilities within the OT environment.		X	X	$764,775
SSZ	6	Enhanced Attack Surface Management & Deception Technology	0.6	Initiative enhances abilities to identify compromises within the environment. Achieved via increasing ability to determine changes to attack surface area and deploying deception technologies.			X	$382,239
SSZ	8	Enhanced Network and Firewall Assurance	0.4	Initiative enhances firewall monitoring, assurance and analysis.			X	$401,544

OT Environment	Initiative	Name	OT CAPEX Factor	Description	Options Applicable			Cost
					Option A	Option B	Option C	
SCADA	2	Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)	0.05	Initiative transitions to enhanced access control of access-on-demand / zero trust model.			X	$142,783
SCADA	3	Enhanced MSSP / IR	0.2	Initiative allows a managed security service provider to continuously monitor all logs within the managed SIEM rather than during business hours only.	X	X	X	$59,400
SCADA	4	Enhanced Identity Governance and Assurance (IGA)	0.075	Initiative allows automated governance processes around access requests, granting access and reviewing access.			X	$281,556
SCADA	5	Enhanced Patch Management	0.125	Initiative enhances patch management capabilities and better enables TransGrid to address vulnerabilities within the OT environment.		X	X	$191,194
SCADA	6	Enhanced Attack Surface Management & Deception Technology	0.15	Initiative enhances abilities to identify compromises within the environment. Achieved via increasing ability to determine changes to attack surface area and deploying deception technologies.			X	$95,560
SCADA	8	Enhanced Network and Firewall Assurance	0.1	Initiative enhances firewall monitoring, assurance and analysis.			X	$100,386