OPTIONS EVALUATION REPORT (OER)

FY24-28 Physical Security Renewals

OER- N2536 revision 0.0

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

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

Approvals

Author	Hazem Khamis	Digital Infrastructure Asset Strategist
Endorsed	Debashis Dutta	Asset Analytics & Insights Manager
	Adam Hoare	Digital Infrastructure Asset Manager
Approved	Lance Wee	Head of Asset Management
Date submitted for approval	29 September 2021	

Change history

Revision	Date	Amendment
0	29/09/2021	First Issue

Executive summary

TransGrid is subject to security risks emanating from several threat sources, all with variable likelihood and consequences. Incidents may range from unauthorised access, vandalism and criminal acts through to sabotage and terrorist acts. It is an inherent obligation of owners and operators of critical infrastructure to effectively manage the security risks to its assets under their control.

Current defect rates are increasing across all security components resulting in extended periods without adequate security coverage to either prevent, detect or review unauthorised access incidents should they occur. Security systems at the 59 identified sites will have reached the end of their serviceable life by FY2023/24.

TransGrid is subject to several legislative, regulatory and safety obligations, including the NSW Electricity Supply (Safety and Network Management) Regulation 2014, the Work Health and Safety (WHS) Regulation 2011 and the currently drafted Security Legislation Amendment (Critical Infrastructure) Bill 2020. These regulations provide minimum standards for public safety and infrastructure security to which TransGrid must adhere. There is therefore a need for TransGrid to address security risks to critical assets under their control.

The assessment of the options considered to address the need/opportunity appears in

Base Case

Under the Base Case TransGrid continues to operate current security systems and undertakes maintenance (O&M) for the sites as required. This approach will not address the health and obsolescence of unsupported security system assets.

Option B — Renewal of Sites to Latest Standards [NOSA N2536, OFS N2536B]

This option involves the replacement of all security systems assets at identified sites. This option will modernise the site security infrastructure to the latest design standards to meet the evolving security risks present to critical infrastructure environments.

Table 1 - Evaluated options

Option	Description	Direct capital cost ($m)	Network and corporate overheads ($m)	Total capital cost[1] ($m)	Weighted NPV (PV, $m)	Rank
N2536B	Renewal of Sites to Latest Standards	2.11	42.39	43.50	4.50	1

This option involves the replacement of all security systems assets at identified sites. This option will modernise the site security infrastructure to the latest design standards to meet the evolving security risks present to critical infrastructure environments.

The preferred option is Option B as it meets the requirements of the need, is the only technically and commercially feasible option that maintains compliance with TransGrid's legislative, regulatory and safety obligations and provides economic benefits to electricity consumers.

[1] 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.

1. Need/opportunity

TransGrid is subject to security risks emanating from several threat sources, all with variable likelihood and consequences. Incidents may range from unauthorised access, vandalism and criminal acts through to sabotage and terrorist acts. It is an inherent obligation of owners and operators of critical infrastructure to effectively manage the security risks to its assets under their control.

The NSW Electricity Supply (Safety and Network Management) Regulation 2014 requires TransGrid to have an Electricity Network Safety Management System (ENSMS), whose primary objective is to ensure that design, construction, commissioning, operation and decommissioning of its network (or any part of its network) is safe. Security systems installed within the network under this project meet the requirements of ENSMS.

The Work Health and Safety (WHS) Regulation 2011 considers TransGrid as a PCBU (person conducting a business or undertaking) and imposes multiple obligations on it in managing risks to health and safety. Under the WHS Regulation, TransGrid as a PCBU has an obligation to ensure that the risk to the health and safety of its workers and members of the public is managed so far as is reasonably practicable.

The currently drafted Security Legislation Amendment (Critical Infrastructure) Bill 2020 is proposing to impose positive security obligations and enhanced cybersecurity obligations onto owners and operators of Critical Infrastructure Assets within Australia. Specifically the Bill imposes a requirement onto such owners and operators as needing to have regard to the National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure[2]. However, this guideline was published in 2006 and, while it has been effective at limiting incidental threats from accessing live electricity infrastructure, it lacks methodology and requirements found in more contemporary standards and frameworks aligned with identification and treatment of sophisticated threats and risk scenarios consistent with Australia's current security landscape. An active ENA working group is currently revising the guideline to address this concern.

TransGrid's Physical Security Design and Construction Manual outlines the minimum standard for security installations at TransGrid network sites and Regional Centres/Depots.[3] The Standard is based heavily on "National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure"[4] and incorporates requirements to secure and protect Critical Infrastructure sites. Due to several risk factors described below, current systems and installations targeted under this compliance need do not meet the Guideline or TransGrid's latest design standards.

There is a compliance need to meet our WHS, ENSMS and currently drafted Security Legislation Amendment (Critical Infrastructure) Bill 2020 obligations by addressing the ageing and obsolete security infrastructure deployments at all identified sites.

A renewal program is required to address the risks presented by:

- End of life assets
- Obsolete and unsupported technology deployments
- Obsolete design philosophies
- Lack of system patching and updates
- Limited security monitoring and response capabilities for unmanned sites
- Lack of system integration

Security systems at the 59 identified sites will have reached the end of their serviceable life by 2023/24.

In accordance with TransGrid's Renewal and Maintenance Strategy for Network Property,[5] a refresh of complete security installations is required. This compliance need arises due to the obsolescence of underlying topology and

[2] ENA DOC 015-2006
[3] Refer to Physical Security Design and Construction Manual
[4] ENA DOC 015-2006
[5] Refer Renewal and Maintenance Strategy – Network Property

security infrastructure that cannot support component upgrades. It is expected that this would provide additional benefits to consumers and the organisation including:

- Achieving greater visibility of sites and improvements in security incident response and action.
- Upgrading to modern design philosophies to reduce operational and maintenance requirements for security systems with the delivery of increased remote interrogation capabilities.
- Offsetting operational costs in corrective maintenance for unsupported technologies.

2. Related needs/opportunities

- There are no identified Needs that would benefit directly from coordination.

3. Options

3.1 Base case

The Base Case for this Need is to continue with TransGrid's business as usual operations and maintenance (O&M) for the sites. This approach does not address the deteriorating condition of security systems at the sites, or the risk cost associated with maintaining obsolete assets. The costs will likely increase due to:

- The probability of failure increasing as assets move further along their failure curves. Failures are the result unrepairable internal electronic subcomponents requiring the replacement of complete assets.
- TransGrid's decreasing ability to recover from asset failure with increasing unavailability of spares or technologically compatible systems over time, which increases the consequence of asset failure.

Key drivers for this increased cost are:

- All targeted assets have reached their end of life and have none or very limited manufacturer support. The underlying technology is no longer produced in the market and thus replacements are reliant on depleting excess stocks of manufacturers or resellers. This increases the likelihood of a hazardous event occurring and decreases TransGrid's ability to mitigate or repair failures.
- Assets have increasing numbers of faults, degrading components or are prone to mechanical wear, increasing the likelihood of a hazardous event occurring.

Increasing maintenance on security systems equipment cannot reduce the probability of failure or reduce risk costs. This is because maintenance of security systems assets can focus on device inspection and functional performance checks only, the conduct of maintenance at an electronic component level is neither feasible nor practicable.

3.2 Options evaluated

Option B — Renewal of Sites to Latest Standards [NOSA N2536 , OFS N2536B]

This option involves replacement of all security systems assets at identified sites. This option will modernise site security infrastructure to the latest design standards to meet the evolving security risks present to critical infrastructure environments.

The condition of various categories of security assets such as CCTV, Access Control and Alarm systems creates a need for modernisation. This will deliver benefits such as reduced preventative maintenance requirements, improved operational efficiencies, better utilisation of TransGrid's high-speed communications network and improved visibility of all assets and security incidents using modern technologies.

There are also additional operational benefits available due to improved remote monitoring, control and interrogation, efficiency gains in responding to faults, and phasing out of obsolete legacy systems and protocols.

This option is planned for deployment across the 2023/24-2027/28 regulatory control period. Targeted assets will be in service for approximately 10 years.

3.3 Options considered and not progressed

Table 2 - Option considered but not progressed

Option	Reason for not progressing
Option A - Individual Asset Replacements	This option involves renewal of individual assets in a like for like manner (old for new). This option does not address infrastructure and design standard obsolescence. Limitations in security capabilities to meet our current security standards and the drafted Security Legislation Amendment (Critical Infrastructure) Bill 2020 cannot be addressed through this option. Therefore, this option does not meet TransGrid's compliance need, as it is not technically feasible.
Asset Retirement	This can only be achieved through retirement of security at all identified sites, which is not technically or commercially feasible.
Non-network solutions	It is not technically feasible for non-network solutions to provide the functionality of security systems assets.

4. Evaluation

4.1 Commercial evaluation methodology

The economic assessment undertaken for this project includes three scenarios that reflect a central set of assumptions based on current information that is most likely to eventuate (central scenario), a set of assumptions that give rise to a lower bound for net benefits (lower bound scenario), and a set of assumptions that give rise to an upper bound on benefits (higher bound scenario).

Assumptions for each scenario are set out in the table below.

Table 3 - Scenarios

Parameter	Central scenario	Lower bound scenario	Higher bound scenario
Discount rate	4.8%	7.37%	2.23%
Capital cost	100%	125%	75%
Operating expenditure benefit	100%	75%	125%
Risk costs benefit	100%	75%	125%
Benefits	100%	75%	125%
Scenario weighting	**50%**	**25%**	**25%**

Parameters used in this commercial evaluation:

Table 4 - Parameters used in commercial evaluation

Parameter	Parameter Description	Value used for this evaluation

Parameter	Parameter Description	Value used for this evaluation
Discount year	Year that dollar values are discounted to	2020/21
Base year	The year that dollar value outputs are expressed in real terms	2020/21 dollars
Period of analysis	Number of years included in economic analysis with remaining capital value included as terminal value at the end of the analysis period.	10 years
Safety disproportionality	Multiplier of the safety risk cost included in NPV analysis to demonstrate implementation of obligation to reduce safety to ALARP.	Refer to section 4.3 for details.

The capex figures in this OER do not include any real cost escalation.

4.2 Commercial evaluation results

The commercial evaluation of the technically feasible options is set out in Table 5. Details appear in Appendix A.

Table 5 - Commercial evaluation (PV, $ million)

Option	Capital Cost PV	Central scenario NPV	Lower bound scenario NPV	Higher bound scenario NPV	Weighted NPV	Ranking
Option B	34.49	1.89	-17.80	32.03	4.50	1

4.3 ALARP evaluation (REPEX Only)

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. Under the Electricity Supply (Safety and Network Management) Regulation 2014 Section 5 'A network operator must take all reasonable steps to ensure that the design, construction, commissioning, operation and decommissioning of its network (or any part of its network) is safe.' TransGrid maintains an Electricity Network Safety Management System (ENSMS) to meet this obligation[6].

In its Network Risk Assessment Methodology, under the ALARP test with the application of a gross disproportionate factor[7], the weighted benefits are expected to exceed the cost. Where TransGrid's analysis concludes that the costs are less than the weighted benefits from mitigating bushfire and safety risks, the proposed investment will enable TransGrid to continue to manage and operate this part of the network to a safety and risk mitigation level of ALARP.

Evaluation of the above options has been completed in accordance with As Low As Reasonably Practicable (ALARP) obligations. The Network Safety Risk Reduction is calculated as 6 x Bushfire Risk Reduction + 6 x Safety Risk Reduction + 3 x other Environmental Risk Reduction + 0.1 x Reliability Risk Reduction.

[6] TransGrid's ENSMS follows the International Organization for Standardization's ISO31000 risk management framework which requires following hierarchy of hazard mitigation approach

[7] In accordance with the framework for applying the ALARP principle, a disproportionality factor of 6 has been applied to risk cost figures. The values of the disproportionality factors were determined through a review of practises and legal interpretations across multiple industries, with particular reference to the works of the UK Health and Safety Executive. The methodology used to determine the disproportionality factors in this document is in line with the principles and examples presented in the AER Replacement Planning Guidelines and is consistent with TransGrid's Revised Revenue Proposal 2023/24- 2027/28.

Results of the ALARP evaluation are set out in Table 6.

Table 6 - Reasonably practicable test ($ million)

Option	Network Safety Risk Reduction	Annualised Capex	Reasonably Practicable?[8]
B	5.03	5.58	No

The result of the ALARP evaluation is that the option is above the ALARP threshold.

4.4 Preferred option

The preferred option to meet the identified need by 2027/28 is Option B. Option B is the only technically and commercially feasible solution to enable TransGrid to continue meeting its obligations set out in the WHS Act (2011), National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure and drafted Security Legislation Amendment (Critical Infrastructure) Bill 2020. Consequently, it will ensure the performance standards applicable to the identified sites' security systems are met.

Option B involves an on-site upgrade and renewal (replacement) of the CCTV, alarm systems, access control and underlying infrastructure at the site to a fully integrated and holistic security platform. Efficiencies will be achieved by reusing available infrastructure where practicable.

Option B is the preferred option in accordance with NER clause 5.15A.1(c) because it is the credible option that maximises the net present value of the net economic benefit to all those who produce, consume and transport electricity in the market. This preferred option, Option B, was found to have a net economic benefit while also maintaining compliance with regulatory and public safety obligations. TransGrid also conducted sensitivity analysis on the net economic benefit to investigate the robustness of the conclusion to key assumptions. TransGrid finds that under all sensitivities, Option B delivers the highest net benefits.

Capital and Operating Expenditure

There is negligible difference in predicted ongoing planned routine operational expenditure between the option and the Base Case.

Resultant corrective maintenance under the base case strategy is anticipated to result in higher expenditure over the upcoming regulatory period. Delivery of proposed works under Option B will reduce the risk of increasing direct defect response costs.

It has been modelled that those components with no manufacturer support and depleting spares carry the potential for incurring aspects of the proposed capital expenditure as operational expenditure. In such a scenario, these higher costs are attributable to significant design and preparation costs, and likely augmentation of linking systems required to move a system from one design solution to a differing solution. Such costs would not be present in cases where a like-for-like replacement is feasible.

These operating expenditure benefits have been captured in the economic evaluation.

Regulatory Investment Test

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

[8] Reasonably practicable is defined as whether the annualised CAPEX is less than the Network Safety Risk Reduction.

5. Optimal Timing

The test for optimal timing of the preferred option has been undertaken. The approach taken is to identify the optimal commissioning year for the preferred option where net benefits (including avoided costs and safety disproportionality tests) of the preferred option exceeds the annualised costs of the option. The commencement year is determined based on the required project disbursement to the meet the commissioning year based on the OFS.

The results of optimal timing analysis is:

- Optimal commissioning year: 2027/28
- Commissioning year annual benefit: $3.81 million
- Annualised cost: $4.13 million

The project is expected to commence in the 2023/24-2027/28 Regulatory Period based on the optimal timing

6. Recommendation

It is the recommendation that Option B – Renewal of Sites to Latest Standards be scoped in detail.

The total project cost is $43.5m including an amount of $8.85m to progress the project from DG1 to DG2.

Appendix A – Option Summaries

Project Description	FY24-28 Physical Security Renewals		
Option Description	Option B - Renewal to latest standards		
Project Summary			
Option Rank	*1*	Investment Assessment Period	*15*
Asset Life	*15*	NPV Year	2020/21
Economic Evaluation			
NPV @ Central Benefit Scenario (PV, $m)	13.16	Annualised CAPEX @ Central Benefit Scenario ($m)	Annualised Capex - Standard (Business Case) 4.13
NPV @ Lower Bound Scenario (PV, $m)	-12.58	Network Safety Risk Reduction ($m)	Network Safety Risk Reduction 5.03
NPV @ Higher Bound Scenario (PV, $m)	55.12	ALARP	ALARP Compliant? Yes
NPV Weighted (PV, $m)	17.21	Optimal Timing	Optimal timing (Business Case) 2023/24
Cost (Central Scenario)			
Total Capex ($m)	43.50	Cost Capex (PV,$m)	34.49
Terminal Value ($m)	0.00	Terminal Value (PV,$m)	0.00
Risk (Central Scenario)	**Pre**	**Post**	**Benefit**
Reliability (PV,$m)	Reliability Risk (Pre) 2.95	Reliability Risk (Post) 1.42	Pre – Post 1.53
Financial (PV,$m)	Financial Risk (Pre) 5.74	Financial Risk (Post) 2.76	Pre – Post 2.98
Operational/Compliance (PV,$m)	Operational Risk (Pre) 0.00	Operational Risk (Post) 0.00	Pre – Post 0.00
Safety (PV,$m)	Safety Risk (Pre) 73.12	Safety Risk (Post) 35.13	Pre – Post 37.99
Environmental (PV,$m)	Environmental Risk (Pre) 0.00	Environmental Risk (Post) 0.00	Pre – Post 0.00
Reputational ($m)	Reputational Risk (Pre) 0.00	Reputational Risk (Post) 0.00	Pre – Post 0.00
Total Risk (PV,$m)	Total Risk (Pre) 81.81	Total Risk (Post) 39.31	Pre – Post 42.50
OPEX Benefit (PV,$m)			OPEX Benefit 0.00
Other benefit (PV,$m)			Incremental Net Benefit 5.15
Total Benefit (PV,$m)			Business Case Total Benefit 47.64

Appendix B Sites Targeted

Substation ID	Substation
AVS	Avon 330kV Switching Station
DNT	Darlington Point Substation
BRG	Buronga Switching Station
BRD	Balranald Substation
BUK	Burrinjuck 132kV Substation
COF	Coffs Harbour Substation
COA	Cooma 132kV (New) Substation
CW2	Cowra Substation
DN2	Deniliquin Substation
GRF	Griffith Substation
GN2	Gunnedah Substation
GTH	Guthega 132kV Substation
HU2	Hume 132kV Substation
INV	Inverell Substation
KVS	Kangaroo Valley Switching Station
KS2	Kempsey Substation
MPP	Mount Piper 132kV Substation
MNY	Munyang Substation
QBN	Queanbeyan Substation
TMW	Tamworth 132kV (New) Substation
TU2	Tumut Substation
ALB	Albury 132kV Substation
MRK	Muswellbrook
FNY	Finley Substation
GNS	Glen Innes Substation
MOL	Molong Substation
PMA	Panorama Substation
BER	Beryl Substation
PMQ	Port Macquarie Substation

Substation ID	Substation
WRH	Waratah West Substation
ANM	Australia News Print Substation
GAD	Gadara 132kV Substation
FB2	Forbes Substation
MRE	Moree Substation
PKS	Parkes Substation
MAN	Manildra 132kV Substation
TRE	Taree Substation
NB2	Narrabri Substation
NAM	Nambucca Substation
TTF	Tenterfield Substation
WWS	Wallerawang 132 (New)
KLK	Koolkhan 132kV Substation
MRU	Murrumburrah Substation
YA2	Yanco Substation
GUR	Gullen Range
CWF	Capital Wind Farm Substation
CLY	Coleambally Substation
TOM	Tomago 132
B0S	Boambee South 132kV Substation
MVL	Macksville 132kV Substation
RAL	Raleigh 132kV Substation
BGE	Boggabri East Switching Station
BGN	Boggabri North Switching Station
NRC	Newcastle Depot
ORC	Orange Depot
SWC	Sydney West Depot
TAC	Tamworth Depot
WRC	Wagga Wagga Depot
YSC	Yass Depot