NEED/OPPORTUNITY STATEMENT (NOS)

Access Card and Intrusion Detection System Replacement

NOS- 000000001595 revision 3.0

Ellipse project no.: P0009474
TRIM file: [TRIM No]

Project reason: Capability - Improved Asset Management
Project category: Prescribed - Security/Compliance

Approvals

Author	Sharmeen Sultana	Professional Engineer
Endorsed	Andrew McAlpine	Asset Performance & Systems Manager
	Azil Khan	Investment Analysis Manager
Approved	Lance Wee	Manager / Asset Strategy
Date submitted for approval	30 November 2016	

Change history

Revision	Date	Amendment
0	10 August 2016	Initial issue
1	29 November 2016	Update to format
2	30 November 2016	Amendment

1. Background

TransGrid is subject to security risks emanating from a number of 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 assets under their control.

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 risk to the health and safety[1]. This regulation is based on The Work Health and Safety (WHS) Act 2011 and is considered legally binding.

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 (SFAIRP). This implies that TransGrid must:

- Identify all reasonably foreseeable risks to the health and safety of its workers and members of the public.
- Identify all control measures which eliminate or minimise the risks.
- Then decide which of the controls are 'reasonably practicable' to be implemented.
- This 'reasonableness of acting' infers that cost solely by itself is unlikely to be a sufficient justification in the court of law for not implementing or lowering a control measure unless the cost is grossly disproportionate to the risk.

TransGrid's Network Security Standard (TRIM No: D2004/2634, Rev 3) outlines the minimum standard for security at TransGrid network sites and Regional Centres/Depots[2]. The Network Security Standard is based heavily on "National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure" (ENA DOC 015-2006). While adopting the ENA guideline, the Network Security Standard remains mindful that the imposed health and safety obligations by the WHS Regulation are met.

Network Security Standard performs site specific security risk assessment for all of TransGrid's substation sites. The risk assessment results into categorisation of each substation sites into "low", "medium", "high" or "critical" risk groupings. The standard then mandates the minimum security treatment required at each sites belonging to these risk groupings.

The main security system works [redacted]. The main security [redacted] and enable System Operations to respond quickly to a verified incident.

Across TransGrid network, [redacted] substations and [redacted] depots have [redacted] local security systems installed. Main security system interfaces with each of these local security systems. The local security system consists [redacted] please see the Attachment 2 for quantity of hardware).

2. Need/opportunity

A gap analysis of TransGrid's existing substation sites for security system has revealed that:

[1] Refer *Work Health and Safety Regulation 2011, part 3.1.* New South Wales. Available at: http://www.legislation.nsw.gov.au/maintop/view/inforce/subordleg+674+2011+cd+0+N. [Accessed 20 January 16].

[2] Refer TransGrid Network Security Standard, *R*ev 3, Section 5.6.

- The manufacturer of our current access card and intrusion detection system has indicated that the mass production of the spare units as well as the hardware/software maintenance support will cease to exist by mid-2020. Meanwhile by 2020, an estimated [redacted] of the access card and intrusion detection system will [redacted] These will expose TransGrid to a significant amount of risk in the areas of physical security, public safety and system reliability if an appropriate action is not considered within a reasonable timeframe.

- This implies that [redacted] as it will be difficult to obtain replacements, spare parts and retain hardware/software support. So [redacted] local security systems are identified for renewal across 98 sites and depots.

- [redacted]

- Inoperability of a main security system implies that the local intrusion detection be inoperative, capability of remote viewing of alarms be lost and remote operating capability of gates and doors be lost from the control rooms and AMC. Loss of such visibility of a site increases the risk of an unauthorised entry.

- The remaining [redacted] sites are also in need of installing security system in order to increase the visibility.

- If the access card and intrusion detection systems at [redacted] substation sites and depot are not replaced, the total risk cost from this asset category that the business will be carrying is $1.53m per annum (see Attachment 1).

Opportunity

- Due to aging, the failure rates of the key components of the security systems will be high and consequently will incur high corrective maintenance cost. It is expected that replacing these security systems with their modern day equivalents will save corrective maintenance cost by approximately $0.32m per annum (based on TransGrid historical maintenance expenditure from July to September 2015.

3. Related needs/opportunities

NIL

4. Recommendation

There are opportunities to reduce risk and save defect maintenance cost by replacing with modern day equivalents.

It is recommended that options be considered to address the identified need/opportunity.

Attachment 1 – Risk costs summary

Summary of results is attached below. Refer to supporting document in PDGS for full risk assessment.

Current Option Assessment - Risk Summary

Project Name: Access card & Intrusion Detection System Replacement

Option Name: 1595 - Base Case

Option Assessment Name: 1595 Base Case - Assessment 1

Rev Reset Period: Next (2018-23)

Major Component	No.	Minor Component	Sel. Hazardous Event	LoC x CoF ($M)	Failure Mechanism	NoxLoC xCoF ($M)	PoF (Yr 1)	Total Risk ($M)	Risk ($M) (Rel)	Risk ($M) (Op)	Risk ($M) (Fin)	Risk ($M) (Peo)	Risk ($M) (Env)	Risk ($M) (Rep)
Security Panel	107	Security Panel	Unauthoried Entry (Security Panel)	$0.05	Failure	$5.54	27.60%	$1.53	$0.23		$1.12	$0.18		$0.00
				$0.05		$5.54		$1.53	$0.23		$1.12	$0.18		$0.00

Total VCR Risk: $0.23 Total ENS Risk: $0.00

The following assumptions are considered to identify the risk cost using investment Risk Tool:

> Probability of Failure (PoF):

- Pre investment POF is calculated based on combination of [redacted] occurred during 2014 – 2015 and also considered that after 2023, the whole fleet [redacted] It implies that the systems will fail to perform their intended task. So the probability that access card and intrusion detection system fails is [redacted] after 2023. So the average rate of failure from 2020 onwards is [redacted]% on average per year.

> Consequences:

- Service Interruption: The LoC for service interruption (electricity) has remained [redacted] for pre investment. This is based on the fact that both a high voltage electrocution/arc and an unauthorised operation of equipment by an intruder will cause a service interruption in the event of main controller failure.
- Personal Injury: The likelihood of consequence (LoC) for personal injury is [redacted] based on rate of unauthorised entry in TransGrid substation sites.
- Repair cost to TransGrid substation asset: It is considered that damage to TransGrid asset caused by intruder would cost $20k considering TransGrid unauthorised entry rate [redacted] per annum.
- Productivity loss: It includes inconvenience to TransGrid staff worth of $18k per annum for each substation site due to faulty access card system and /or main security system.

Attachment 2 - High level Scope of Work

Table 1 depicts the associated key component that needs to be replaced as part of access card and intrusion detection system replacement. Across TransGrid network, there are [redacted] local security systems currently in place covering [redacted] substations and [redacted] security systems covering [redacted]. [redacted] of the substation sites do not have any security systems installed. So as part of this need, [redacted] local security systems at [redacted] sites and depots are to be replaced and nine (9) new security systems to be installed at [redacted] sites.

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]