NEED/OPPORTUNITY STATEMENT (NOS)

Motion Detector Replacement

NOS- 000000001452 revision 3.0

Ellipse project no.: P0008469
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
Approved	Lance Wee	Manager / Asset Strategy
Date submitted for approval	30 November 2016	

Change history

Revision	Date	Amendment
0	4 May 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 the security risks to its 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). This is a guideline produced by Energy Network Association to be used as a tool that promotes an understanding of safety and security issues and outlines a number of control measures in order to achieve protection against security threats and public safety incidents around electricity infrastructure. 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.

TransGrid substation sites have multiple security controls/treatments currently in place which [redacted]

2. Need/opportunity

A motion detector is an electronic device that detects movement within the secure perimeter of a substation and sends alarm to the control centres [redacted]. Motion detectors form part of the Access Card and Intrusion Detection system and are generally installed within the [redacted]

[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*, Rev 3*, Section 5.6.

[redacted]. The system is designed to detect an intrusion [redacted] The selection of detector is dependent on the object, space or perimeter to be protected. TransGrid uses [redacted] technology as this provides a [redacted] vertically and is one of the approved devices in accordance with Australian standards.

A gap analysis of TransGrid's existing substation sites against the Network Security Standard has revealed that:

> [redacted] is expected that replacing these detectors with their modern day equivalents will reduce [redacted] maintenance cost by approximately $0.004m per annum based on historical maintenance expenditure.

> [redacted] and expected to reduce [redacted] by $0.015m per year.

> [redacted]

> A defective detector may result in a genuine intrusion to remain undetected, which exposes TransGrid to the risk of an unauthorised entry. An unauthorised entry to a substation site can potentially lead to the following consequences;

- Safety incident such as, personal injury or fatality arising from electrocution, electric shock or arc burns. On 15 June 2001, a 12-year-old boy was electrocuted when he came into contact with live bus bars and died as a result after he entered the Ausgrid Cronulla Substation[3].
- Trip of substation equipment(s) resulting from a safety incident or unauthorised operation of equipment. It may cause interruption of electricity supply to the customers. On 31 August 2006, an intruder gained entry through a hole in the switchyard perimeter fence at Ingleburn Substation and operated a 330kV circuit breaker based on TransGrid Incident Notification System (INS) report.
- The risk cost is $0.73m per annum if nothing is done at [redacted] substation sites with regards to installing motion detector (see Attachment 1).

3. Related needs/opportunities

NIL

4. Recommendation

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

[3] Refer www.smh.com.au. 2003. *Electrocuted boy invited friends to play in cubby he built next to substation*. [ONLINE] Available at: http://www.smh.com.au/articles/2003/02/24/1046063962028.html. [Accessed 20 January 16].

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: Motion Detector Replacement

Option Name: 1452 - Base Case

Option Assessment Name: 1452 - 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)
Motion Detector	44	Detection	Unauthoried Entry (Motion Detector)	$0.03	Failure	$1.49	49.00%	$0.73	$0.17		$0.43	$0.13		$0.00
				$0.03		$1.49		$0.73	$0.17		$0.43	$0.13		$0.00

Total VCR Risk: $0.17

Total ENS Risk: $0.00

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

- Probability of Failure (POF):
  - Probability that motion detector may fail is [redacted] based on TransGrid historical data.
- Consequences:
  - **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 per annum.
  - **Service Interruption:** The LoC for service interruption (electricity) is assumed to be 1%. This is based on the fact that both a high voltage electrocution/arc flash and an unauthorised operation of equipment by an intruder will cause a service interruption.