NEED/OPPORTUNITY STATEMENT (NOS)

Physical Security of Comms Equipment

NOS- 000000001583 revision 1.0

Ellipse project no: P0009382
TRIM file: [TRIM No]

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

Approvals

Author	Mark Jones	Secondary Systems and Communications Asset Manager
Endorsed	Adam Hoare	Senior Secondary Systems Analyst
Approved	Lance Wee	M/Asset Strategy
Date submitted for approval	30 November 2016	

Change history

Revision	Date	Amendment
0	1 November 2016	Initial issue
1	30 November 2016	Update to format

1. Background

TransGrid substations and radio repeater sites all have telecommunications equipment that provide access into various corporate and operational networks that TransGrid relies upon to carry out its functions. The sites that this equipment is housed at are unmanned and have relied upon the measures in place for the high voltage transmission network to provide physical security for the operational and corporate data networks.

As the potential to disrupt TransGrid operations via a cyberattack increases as operational and information technology systems converge, the value in providing a higher level of physical security at unmanned sites will be reviewed.

2. Need/opportunity

TransGrid runs its infrastructure without the need for a constant presence at all of its sites. Access is provided to staff and contractors to perform their duties at these sites.

Access into a substation or a radio repeater site provides access to data networks and associated equipment that are critical for managing TransGrid's operations. Interference with these systems, whether unintentional or malicious, could have widespread effects to TransGrid's Corporate Data or Operational Systems.

TransGrid can install locked doors on the cabinets housing this equipment to provide greater certainty of the security of this equipment.

The risk cost associated with this need is $400k per annum. The most significant element of concern is a Service Failure caused by an inadvertent action. The risk costs are based on 2015/16 probabilities of failure and the Borg Scale methodology of assessing IT network and cyber security risk.

3. Related needs/opportunities

Nil

4. Recommendation

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: Physical Security of Comms Equipment

Option Name: 1583 - Base Case

Option Assessment Name: Copy of 1366 - Option 1 - Assessment 1

Rev Reset Period: Next (2018-23)

Major Component	No.	Minor Component	Sel. Hazardous Event	LoC x CoF ($M)	Failure Mechaniam	NoxLoC xCoF ($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)
Comms Equipment	100	Distribution	Service Failure (Comms Equipment)	$399.98	Security Vulnerability	$39,998.08	0.00%	$0.40	$0.40		$0.00	$0.00	$0.00	$0.00
Comms Equipment	100	Distribution	Unapproved Change (Comms Equipment)	$399.98	Security Vulnerability	$39,998.08	0.00%	$0.00	$0.00		$0.00	$0.00	$0.00	$0.00
				$799.96		$79,996.16		$0.40	$0.40		$0.00	$0.00	$0.00	$0.00

Total VCR Risk: $0.40 Total ENS Risk: $0.00