Program of Works

2017 – 2022

Safety and Security of Communications Assets (PUBLIC VERSION)

Document number	N/A
Issue number	1
Status	Approved
Approver	E. Viel
Date of approval	April 2015

ISSUE/AMENDMENT STATUS

Issue No	Date	Description	Author	Approved
1	June 2015	Initial draft issue	A. Nainhabo	E. Viel

Disclaimer

This document belongs to AusNet Services and may or may not contain all available information on the subject matter this document purports to address. The information contained in this document is subject to review and AusNet Services may amend this document at any time. Amendments will be indicated in the Amendment Table, but AusNet Services does not undertake to keep this document up to date.

To the maximum extent permitted by law, AusNet Services makes no representation or warranty (express or implied) as to the accuracy, reliability, or completeness of the information contained in this document, or its suitability for any intended purpose. AusNet Services (which, for the purposes of this disclaimer, includes all of its related bodies corporate, its officers, employees, contractors, agents and consultants, and those of its related bodies corporate) shall have no liability for any loss or damage (be it direct or indirect, including liability by reason of negligence or negligent misstatement) for any statements, opinions, information or matter (expressed or implied) arising out of, contained in, or derived from, or for any omissions from, the information in this document.

Contact

This document is the responsibility of Asset Engineering – Asset Management Division, AusNet Services. Please contact the indicated owner of the document with any inquiries.

Edoardo Viel

AusNet Services

Level 31, 2 Southbank Boulevard

Melbourne Victoria 3006

Ph: (03) 9695 6000

Table of Contents

1 Summary

PROGRAM	Site security and implement best practice cyber security standards
SERVICE DATE	On-going throughout period 2018 – 2022
LOCATION	Various Victorian electricity transmission network communications installations
VALUE	$ 3.75M

FY17/18	FY18/19	FY19/20	FY20/21	FY 21/22	Total
$1,333k	$283k	$755k		$1,378k	$3,749k

This works program document should be read in conjunction with the Communication Systems Asset Management Strategy[1] which provides details of the services offered, asset age and condition, key issues, requirements, and the strategies.

2 Program Scope

This program is aimed at improving and enhancing the physical and cyber security of the communication network assets. The proposed improvements will align the management of the communication assets with the AusNet Services Mission Zero principles.

Physical security and safety is aimed at addressing issues at [C.I.C] sites. The scope of work is mainly to enhance the current physical security and safety of the sites.

Computer security will focus on all the sites with communication network assets and similar to physical security the aim is to enhance the current computer security method.

2.1 Physical Security and Safety

2.1.1 Earthing

Improve earthing of radio infrastructure at 31 radio communication sites (Appendix A – Table 1).

2.1.2 Physical Security

Install [C.I.C] at 31 [C.I.C] communication sites (Appendix A – Table 1).

[1] AMS 10-56 Communication Systems

2.2 Computer Security

2.2.1 Implementing Terminal Station Security Architecture

- Design and implementation of [C.I.C] security zones.
- Software licensing for management and monitoring;
- Configuration and testing.

2.2.2 Implementing Authentication and Access controls for the ICS devices

- Implement [C.I.C] devices.

2.3 Project Budget

	Amount $
Physical site security and safety	[C.I.C]
Computer Security Systems	[C.I.C]
Total	**3,749,000**

3 Project Drivers

Implementation of this program of work will enable AusNet Services to economically address the following business drivers:

3.1 Safety

- Industry leadership in safety performance:
  - Minimise electricity transmission network associated risks to employees, contractors and the general public by enabling safe remote monitoring and control of network assets.

3.2 People

- High performing leadership, capability and culture:
  - N/A.

3.3 Financial

- Sustainable earnings and security holder value growth:
  - Reduce the risk of widespread power outages caused by failure of [C.I.C] systems.
- Expansive and accretive growth:
  - N/A.

3.4 Business and Asset

- Safe, resilient and reliable networks.
  - Comply with the National Electricity Rules (NER) by ensuring:
    - ❖ Power transfer is not constrained because of communication systems;

    - ❖ The system is available at all times except for short periods (up to 8 hours) of time for maintenance;
    - ❖ Data transfer from power stations and terminal stations meets Australian Energy Market Operator (AEMO) requirements.

- – An efficient business model supported by intelligent, automated and integrated processes and systems:
  - ▪ The communications network continues to efficiently provide services that incorporate existing requirements while accommodating new technological evolution.
- – Industry leadership and advocacy role in regulatory development;
  - ▪ N/A.

3.5 Customer

- – A highly developed customer service capability;
  - ▪ N/A.

4 Overview

Communications radio sites are typically located in [C.I.C] areas. Access security is maintained by using [C.I.C] for entry into the site and building. Many of the sites are [C.I.C] which have equipment installed in either separate buildings or in the same building as AusNet Services. The [C.I.C] arrangement with [C.I.C]and lack of a standardised security implementation at the [C.I.C] sites exposes the communication network to risks which could impact the operation of the Victorian electricity transmission network.

Cyber security of critical infrastructure such as power utilities is a sensitive matter for governments and regulators. Industrial Control Systems (ICS) may be targeted by malicious individuals for a range of reasons including financial gain, corporate espionage, or terrorist activities. To avoid the risk of being a target, AusNet Services' Information Security is focussed on ensuring that new deployments are implemented with adequate security controls, and that existing controls are adequate to protect against current threats.

In the event of an attack, the goal of cyber-security infrastructure and controls is to quickly identify the issue, contain the breach, and recover to normality so that the damage or outage to the electricity network is minimised. Until recently, standard [C.I.C] were considered sufficient to defend against most cyber-attacks. However, over the past two years, attack sophistication has increased many fold and newer and smarter technologies are required to combat ever increasing threats of an attack. Attacks are now covert in nature and the perpetrators take a long time to infiltrate computer networks to evade detection from the security monitoring tools and controls. To detect such attacks, [C.I.C].

To minimise the risk of a cyber-attack, this program [C.I.C].

5 Risk Analysis

5.1 External Risks

5.1.1 Political, Regulatory and Statutory

- Breach of power system protection and operational requirements.

5.1.2 Physical

- Exposure of AusNet Services' assets to vandalism and theft.

5.1.3 Technology

- [C.I.C].

5.2 Internal Risks

5.2.1 Process and Services

- Unauthorised access to the [C.I.C] network;
- Failure to meet customer requirements.

5.2.2 Strategy

- Users not provided with the appropriate communication network services.

5.2.3 Business Performance

- Accessing [C.I.C] and impacting other corporate activities.

5.2.4 Stakeholder Management

- Failure to meet customer requirements;
- Provision of inadequate customer service.

5.2.5 Data/Information

- Loss of confidential information and intellectual property;
- Failure to meet availability targets.

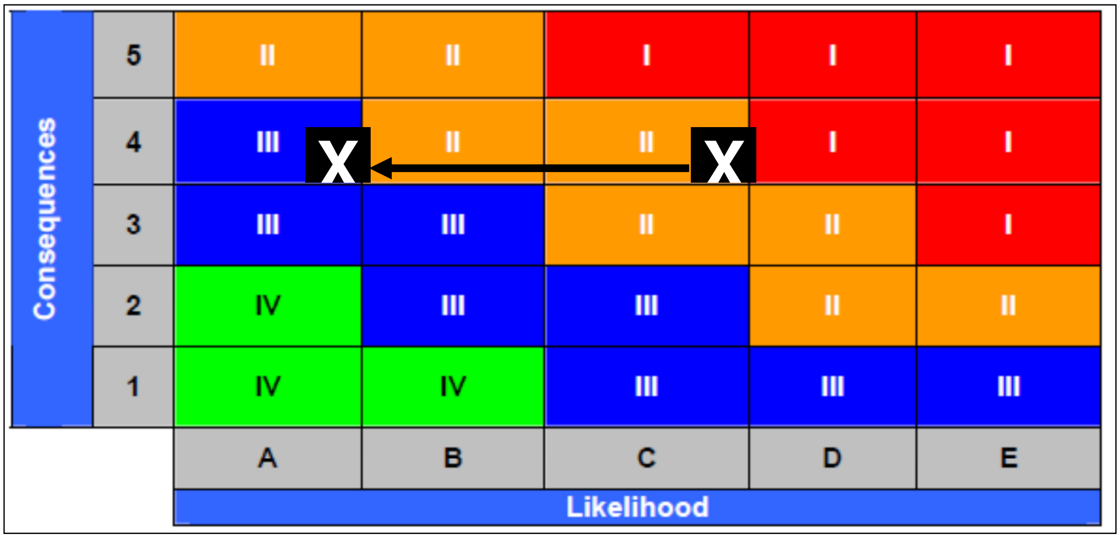
5.3 Summary Risk Assessment

The risks associated with the current state of computer security controls are summarised as follows:

- Unauthorised access to the [C.I.C];
- Disruption of the delivery of electricity to customers; and
- Cyber-attack going unnoticed.

Table 2 in Appendix B shows the risk evaluation using the AusNet Services' Risk Matrix[2] (Corporate Risk Management Framework V3.0 RM 001-2006).

The figure below shows the current risk level and the risk level after completion of the program of works.



Consequences					
5	II	II	I	I	I
4	III X	II	II X	I	I
3	III	III	II	II	I
2	IV	III	III	II	II
1	IV	IV	III	III	III
	A	B	C	D	E
	Likelihood				

Figure 1 – Risk level before and after Program of Works

6 Options

Option 1 Business as Usual

Option 2 Planned Safety and Security Improvements

6.1 Option 1 – Business as Usual

A "Business as Usual" option operates and maintains the existing security controls until equipment failure or successful attack and [C.I.C]. [C.I.C]. No replacements are planned. Site physical security continues to use [C.I.C] systems.

6.2 Option 2 – Improve Safety and Security

Establishment of an improvement program targeting most vulnerable sites:

- Extend monitoring functionality to [C.I.C] devices;
- Implement an architecture that [C.I.C];
- Implement [C.I.C] systems to maintain site physical security.

[2] AusNet Services Risk Management Framework – RM 001-2006

7 Options Analysis

7.1 Option 1 – Business as Usual

This option fails to address any of the key business drivers in section 3. The 'Business as Usual' approach exposes AusNet Services to significant financial and regulatory risk by failing to demonstrate an appropriate level of due diligence. Unauthorised access to the network can present potentially significant health and safety issues. Entry into a communication site can also present risks with operating the electricity network.

This option is inconsistent with AusNet Services' obligations under the Electricity Safety Act, the Occupational Health and Safety Act, accepted Electricity Safety Management Scheme, and obligations under the National Electricity Rules to maintain the quality, reliability and security of supply of prescribed transmission services.

7.2 Option 2 – Planned Safety and Security Improvement

This option addresses the identified key business drivers. Access to the [C.I.C] devices will be constantly monitored and logged. The [C.I.C] will be separated from the corporate network and any suspicious traffic investigated. Access to communication sites will be regularly monitored and controlled.

8 Financial Analysis

The options have been analysed using the corporate NPV model. The benefits and costs of each option are based on an estimate from the corporate risk model.

	Economic Least Cost Analysis				Financial Return		
Analysis of Investment Options ($'000s)	**PV Capital Cost**	**PV Opex Costs**	**PV Community Costs & Benefits**	**Total PV Cost**	**NPV including Reg Return (post tax)**	**PV Cost Ratio**	**PV of Incentive / (Penalty)**
Business As Usual	-	(22)	(18,273)	**(18,295)**	-	1.00	-
Improve Safety and Security of the Network	**(3,496)**	**-**	**-**	**(3,496)**	**47**	**159.45**	**-**
	-	-	-	**-**	-	-	-
	-	-	-	**-**	-	-	-
	-	-	-	**-**	-	-	-

All figures are in $000's unless otherwise stated.

8.1 Option 1 – Business as Usual

Business as usual option will lead to complete loss of communication and failure to operate the electricity network.

PV of Capex and Opex	• No CAPEX however some OPEX to supervise site physical access at the [C.I.C].
PV of Community Costs & Benefits	• A cyber-attack could lead to a safety and health incident that may result in a death or serious injury. The attack could lead to [C.I.C]. Such incidents will lead to increased scrutiny from the regulator, litigation by injured people, undue press coverage and loss of stakeholder confidence in the company.

8.2 Option 2 – Planned Safety and Security Improvement

The selective improvement of security allows AusNet Services to minimise the possibility of a [C.I.C] and consequently the costs associated with such an event.

PV of Capex and Opex	• The OPEX spend associated with supervising [C.I.C] is avoided because the gates are [C.I.C].
PV of Community Costs & Benefits	• This option will avoid the costs associated with the business as usual option.

9 Recommended Action

Option 2 (Planned Safety and Security Improvement) is recommended.

10 Reference Documents

- Electricity Safety Act.
- Occupational Health & Safety Act – provision of safe work environment.
- AEMC National Electricity Rules (version 71).
- AMS – Victorian Electricity Transmission Network – Communications Systems (AMS 10-56).
- AMS – Victorian Electricity Transmission Network – Asset Life Evaluation (AMS 10-101).
- Asset Management Strategy for the Victorian Electricity Transmission Network (AMS 10-01).

Appendix A: Radio Communication Sites

Business	Location type	Code	Name
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]

Business	Location type	Code	Name
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]
Transmission	Radio Station	[C.I.C]	[C.I.C]

Table 1 – List of Radio Sites

Appendix B: Risk Register Template

Entity/Project: ____________ **Facilitator:** [C.I.C] **Date:** ____________

RISK IDENTIFICATION			RISK TREATMENT			RISK ANALYSIS						
						Residual Risk				Target Risk		
Risk	Causes	Impacts	Controls (Current)	RCE	Treatment Actions (Future)	Conseq Rating	Like. Rating	Residual Risk Rating	Project Financial Exposure (Residual)	Conseq Rating	Like. Rating	Target Risk Rating
[C.I.C]	[C.I.C]	Health and Safety • Uncontrollable network leading to injury Environment and Community • Reputation • Regulation • Legal and Compliance • Internal complaints and litigation	• Operational processes • Physical security	Very Poor	• [C.I.C]	3	C	II	$1M	3	B	III
[C.I.C]	[C.I.C]	Health and Safety • Uncontrolled network could lead to death Environment and Community • Loss of power supply • Oil spills Reputation • Undue press coverage • Unreliable asset managers Regulation • More scrutiny from the regulator Legal and Compliance • Class action • fines	• [C.I.C] • Operational processes • Physical security	Requires improvement	• [C.I.C]	4	C	II	$10M	4	A	III

RISK IDENTIFICATION			RISK TREATMENT			RISK ANALYSIS						
						Residual Risk				Target Risk		
Risk	Causes	Impacts	Controls (Current)	RCE	Treatment Actions (Future)	Conseq Rating	Like. Rating	Residual Risk Rating	Project Financial Exposure (Residual)	Conseq Rating	Like. Rating	Target Risk Rating
[C.I.C]	• [C.I.C]	Health and Safety • Inability to control the electricity network Environment and Community • Reputation • Press coverage Regulation • Legal and Compliance • Due diligence	• [C.I.C]	Uncontrolled	• [C.I.C]	3	C	II	$1M	3	B	III

Table 2 – Risk Evaluation Table