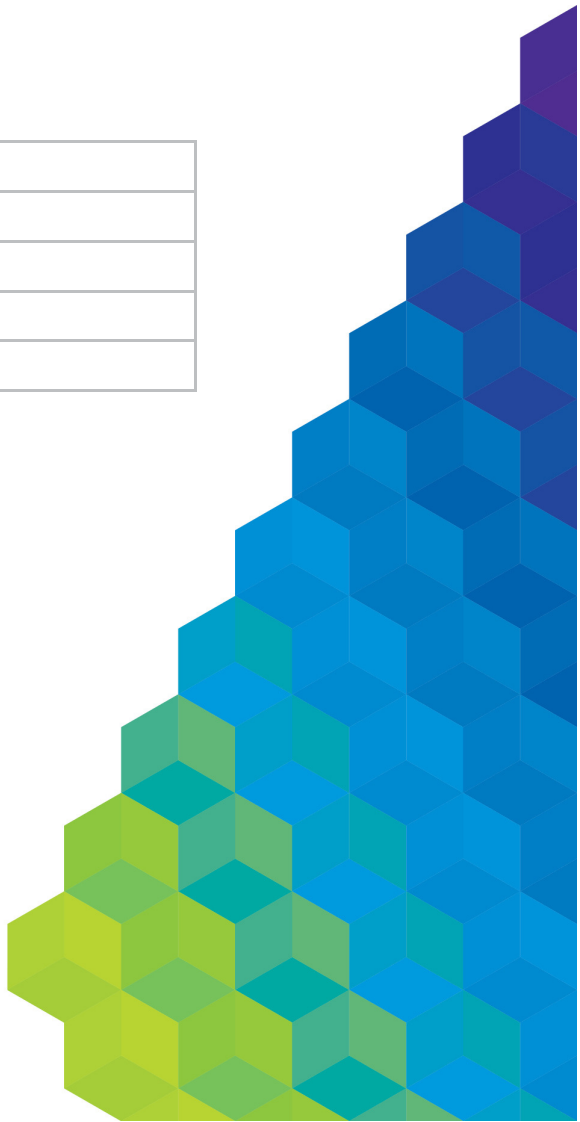
Program of Works

2017 – 2022

Security System Infrastructure Replacement (PUBLIC VERSION)

Document number	N/A
Issue number	1.0
Status	Approved
Approver	S. Owens
Date of approval	03/07/2015



ISSUE/AMENDMENT STATUS

Issue Number	Date	Description	Author	Approved by
0.1	24/03/15	Initial draft	S. Goel	S. Owens
1.0	03/07/15	Initial Issue	S. Goel	S. Owens

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 the Asset Management Division, AusNet Services. Please contact the indicated owner of the document with any inquiries.

Steve Owens

AusNet Services

Level 31, 2 Southbank Boulevard

Melbourne Victoria 3006

Ph: (03) 9695 6000

Table of Contents

1 Summary

PROGRAM	Infrastructure Security Systems (ISS) Capital Replacement Program 2017/18 – 2021/22.
SERVICE DATE	On-going throughout period 2017/18 – 2021/22.
LOCATION	Various Terminal Stations across Victoria.
VALUE	$12.5M.

Table 1 – Program Overview

This works program document should be read in conjunction with AMS 10-63 Infrastructure Security. AMS 10-63 details the background and the strategies for risk mitigation associated with infrastructure security

1.1 Program Scope

The scope for replacement/upgrade of Infrastructure Security Systems (ISS) program covers following works:

- [C.I.C]
- [C.I.C]
- [C.I.C]
- [C.I.C]
- [C.I.C]
- [C.I.C]

1.2 Program Expenditure Forecast

2016/17 ($k)	2017/18 ($k)	2018/19 ($k)	2019/20 ($k)	2020/21 ($k)	2021/22 ($k)	Total ($k)
1,000	2,500	2,500	2,500	2,500	2,500	13,500

Table 2 – Program timing and forecast expenditure

The total program is $13.5M; however, $1M of work is scheduled for the 2016/17 financial year meaning a total of $12.5M is scheduled for the 2017-22 regulatory period.

Forecast costs shown in Table 2 are $2014/15 P50 direct costs. These costs exclude overheads, finance charges and cost escalation.

2 Program Drivers

Assessments of security risk at various terminal stations sites and asset condition of ISS assets have revealed that several terminal stations do not have appropriate security. This exposes the assets to credible threats and potential security incidents.

The program is driven by the need to mitigate the effects of security incidents by:

- Ensuring that only authorised and appropriately trained personnel have access to assets
- Preventing unauthorised access
- Preventing the loss of asset functionality for the community, clients and customers,
- Identifying and responding to security incidents
- Minimising the impact of security incidents

3 Obligations

There are numerous obligations that AusNet Services must comply with, which includes, but not limited to the National Electricity Rules, the Electrical Safety Act, the Occupational Health and Safety Act 2004 (Vic), Terrorism (Community Protection) Act 2003 and the Emergency Management Act 1986.

The National Electricity Rules require AusNet Services to forecast operating and capital expenditures to, amongst other objectives, *comply with all applicable regulatory obligations or requirements associated with the provision of prescribed transmission services* and *maintain the quality, reliability and security of supply*[1]

The Electricity Safety Act requires a major electricity company, such as AusNet Services to *design, construct, operate, maintain and decommission its supply network to minimise as far as practicable—*

(a) the hazards and risks to the safety of any person arising from the supply network; and

(b) the hazards and risks of damage to the property of any person arising from the supply network; and

(c) the bushfire danger arising from the supply network.[2]

In the definitions of this Act, the term 'practicable', *means practicable having regard to—*

(a) the severity of the hazard or risk in question; and

(b) the state of knowledge about the hazard or risk and any ways of removing or mitigating the hazard or risk; and

(c) the availability and suitability of ways to remove or mitigate the hazard or risk; and

(d) the cost of removing or mitigating the hazard or risk;[3]

This means "as low as reasonably practicable" which has been interpreted as until the safety related costs are (grossly) disproportionate to the safety related benefit.

The *Occupational Health and Safety Act 2004* (Vic) (**OHSA**) requires AusNet Services to, *as far as is reasonably practicable, provide and maintain for employees of the employer a working environment that is safe and without risks to health.*[4]

1 National Electricity Rules, Chapter 6A 6.6, 6.7.

2 Electricity Safety Act 1998, clause 98.

3 Electricity Safety Act 1998, Part 1, Definitions.

4 Occupational Health and Safety Act 2010, Section 21(1).

When determining what is (or what was, at a particular time), reasonably practicable in ensuring health and safety, the OHSA requires that regard be had to the following matters:

a) *the likelihood of the hazard or risk concerned eventuating;*
b) *the degree of harm that would result if the hazard or risk eventuated;*
c) *what the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing the hazard or risk;*
d) *the availability and suitability of ways to eliminate or reduce the hazard or risk.*[5]

In acknowledging these obligations AusNet Services has integrated the security practices of its electricity transmission, electricity distribution, and gas distribution businesses to ensure that the diverse threats of unauthorised, malicious, criminal and terrorist intrusion upon assets are consistently identified and addressed.

Several assets under ISS require upgrade / replacement due to various reasons in order to maintain acceptable levels of risk. Major failure of ISS can result in the following:

- Health and Safety incidents.
- Intentional or unintentional asset damages.
- Financial penalties.
- Significant repair costs.
- Severely constrained system capacity.

As AusNet Services is a "*declared essential service provider*[6]", there are a number of obligations that address Legislation and Australian Standards and Guidelines. Specific requirements include risk management, alarms, lighting, fencing, signage, CCTV, site maintenance / natural surveillance, electronic access systems, locks, keys and building security.

Implementation of this program of work will assist AusNet Services in addressing the following business drivers:

- Safety of employees, contractors and the general public:
    - Minimise risk to public due to improved effectiveness of ISS systems and minimised unauthorised entry.
- Financial risk:
    - Reduce capital and operating costs through intentional or unintentional asset damage control.
    - Reduce financial penalties associated with poor asset availability.
    - Reduce civil actions resulting from personal injury/compromised health.
- Regulatory compliance:
    - Victorian Terrorism (Community Protection) Act 2003.
    - Infrastructure security safety guidelines from Electricity Network Association (ENA).
    - Occupational Health & Safety Act (provide safe work environment).
- Corporate image maintained as prudent asset managers:
    - Manage risk of unauthorised entry and asset damage to as low as practicable.

[5] Occupational Health and Safety Act 2010, section 20(2).

[6] Terrorism (Community Protection) Act 2003, Part 6

4 Overview

Infrastructure Security Systems (ISS) protect AusNet Services' assets from unauthorised entry (with or without malicious intentions) into the terminal station and control buildings. Unauthorised entry could result in significant damage to assets (intentional or unintentional) impacting system security and the security of supply or personal injury.

A rise in global terrorism has led the Commonwealth and State governments to impose legal responsibility on the owners and operators of critical infrastructure, such as electricity transmission installations to take all necessary preventative security measures to ensure the continuity of supply. The Victorian Terrorism (Community Protection) Act 2003 requires electricity and gas providers to develop and monitor risk management plans – including all appropriate preventative security and emergency restoration measures.

The Commonwealth and State Governments have designated selected electricity transmission sites as critical infrastructure.

AusNet Services maintains more than 75 transmission installations that are subject to security provisions, including terminal stations, equipment fences inside terminal stations, and depots. Relevant assets include more [C.I.C] to the Customer Energy Operations Team (CEOT).

5 Risk analysis

5.1 Risks and treatment measures

AusNet Services has assessed the criminal, malicious, terrorist and unauthorised access security risks for electricity transmission sites. Please refer to AMS 10 – 63: Infrastructure security for further details.

All the terminal stations and other related sites have been ranked in three categories according to the security risk levels. Table 3 provides the summary of number of sites with each risk level along with a description of the required security measures.

AusNet Services started major infrastructure security upgrades approximately ten years ago. Since 2004 all the highest priority risk sites [C.I.C] have been addressed and installed with most of the security upgrades, including [C.I.C]. Also, [C.I.C] sites security fences have been upgraded by installation of [C.I.C] as they are further secured by [C.I.C] fences.

Victoria police has also recommended [C.I.C] as high security risk, which are included in RL1 list.

Among RL1 security sites, [C.I.C] have been installed with [C.I.C] (Table 3) since 2004. However, the majority of [C.I.C] initially installed are now outdated and have reached end of service life demonstrated by the failure of several [C.I.C]. Additionally several sites in the highest risk category still require the installation of [C.I.C] to be consistent with other utilities in terms of security measures.

Another area requiring major upgrade work at RL1 sites is [C.I.C], which dates back to the original installation of the station. The majority of [C.I.C] is outdated and inefficient [C.I.C] and ongoing maintenance requirements. A major upgrade of [C.I.C] has been proposed in conjunction with [C.I.C] to maximise the security effectiveness and delivery efficiencies during the forecast regulatory period. In the first phase, all the highest security stations will be targeted followed by RL2 and RL3 sites in future programs that extend beyond the forecast regulatory periods.

The majority of ISS assets, at medium and low risk sites (RL2 and RL3), are the original installations and require upgrade to comply with AusNet Services' security policy. Approximately [C.I.C] of the security fences at RL2 sites have been upgraded since 2004 by modification to meet the new standard by installation of a

[C.I.C] and replacement of [C.I.C] . The remaining [C.I.C] sites are in poor condition and require complete replacement/upgrade.

Risk Ranking	Description of works / Issues	Number of Terminal Stations and other related sites*
Risk Level 1 (RL1)	[C.I.C]	[C.I.C]
	[C.I.C]	[C.I.C]
	[C.I.C]	[C.I.C]
Risk Level 2 (RL2)	[C.I.C]	[C.I.C]
Risk Level (RL3)	[C.I.C]	[C.I.C]

**Communication sites have been excluded from the table.*

Table 3 – Number of terminal stations with associated risks

Economic evaluations by NPV modelling (AusNet Services' financial assessment tool) has been performed in conjunction with risk assessments to establish that the proposed upgrade / replacement program of ISS assets is financially / economically justified. This program of work will remove significantly the existing risk associated with major failure of ISS assets during any security threat incident.

5.2 Risk Matrix

The ISS upgrade / replacement program will significantly reduce the likelihood of a major security asset failure during any security threat incident. This reduction in likelihood will be achieved by replacing / upgrading ISS assets which are in poor condition or non-compliant. Upgrades also include the installation of new technological measures if available and proved prudent to be installed. The integrated use of several latest technology measures in coordination to each other shall ensure the required level of security. The continuation of the program is recommended to ensure levels of risks remain below acceptable limits into the future. Implementation of the ISS upgrade/ replacement program aims to move security risks in the direction of the arrow shown in Figure 1. This will result from a reduction in both the likelihood of an event (using deterrents such as [C.I.C]) and consequence (using [C.I.C] to quickly respond to intrusions).

The majority of systems / assets shall be compliant to current Australian Standards and security guidelines reducing significantly the risk of any major asset damage, financial penalties, or compensations. With effective ISS systems, the possibility of any security related incident shall be reduced significantly resulting in a reduction in asset damage, OHS risks and negative impact on community.

Further detail of the security risk associated with terminal stations is detailed in AMS 10-63.

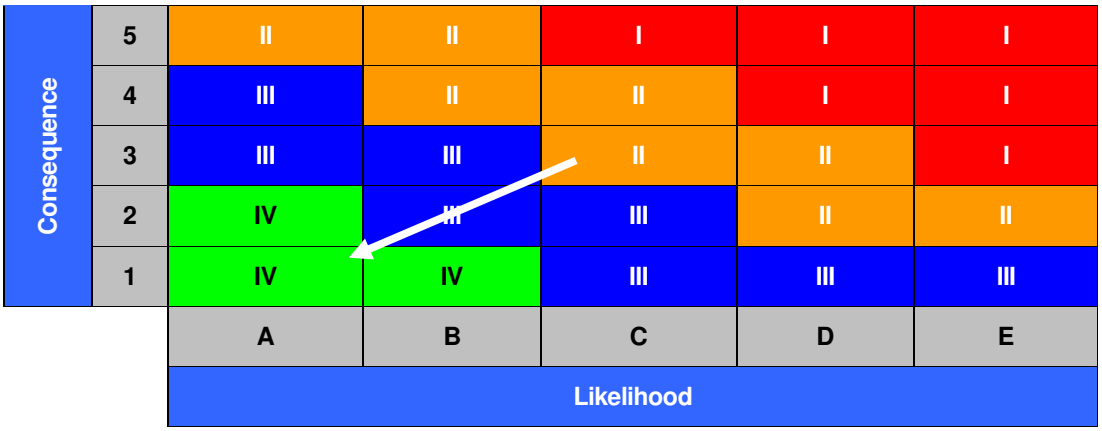


Figure 1 – Risk Matrix

6 Options

Option 1 Do Nothing

Option 2 Replace on Condition

Option 3 Replace on Age

Each of the options has been evaluated against the key criteria of regulatory compliance, Australian Standards, state directives, OH&S and asset damage/theft. This analysis is shown in Table 4.

	RISK TREATMENT REMARKS			
Option	**Regulatory Compliances**	**Australian Standards / State Directives**	**OH&S and Asset Damage / theft**	**Net Present Cost**
Option 1	No	No	No	Highest
Option 2	Yes	Yes	Yes	Lowest (Recommended)
Option 3	Yes	Yes	Yes	Second Highest

Table 4 – Summary of option analysis

6.1 Option 1 – Do nothing

The "Do Nothing" option involves:

- continuing inspection and maintenance activities for ISS assets;
- repairing failed components during inspections or identified as defective;
- continue with non-compliant / aged / outdated and progressively non-functional assets;
- progressive loss of functionality and hence exposure to increasing infrastructure security risks, including loss of service to consumers.

The "Do nothing" involves routine inspection and maintenance but takes no action to proactively refurbish or replace assets as they deteriorate and ultimately fail. In this option the functionality of the assets is progressively lost. This option involves accepting risks associated with aged and non-compliant assets assessed with several issues. Choosing Option 1 will not assist with reducing risks and will not assist with maintaining acceptable levels of risks into future.

This option does not address AusNet Services' obligations under the National Electricity Rules and obligation to Central or State directive or guidelines. Additionally this option doesn't align with best industry practice and significantly impact the reputation of the company in case of any security related incident or public safety incident.

This option is inconsistent with the requirements of the Electricity Safety Act and AusNet Services' accepted Electricity Safety Management Scheme.

6.2 Option 2 – Risk based replacement program

Implementing a condition/ risk assessment based replacement program involves:

- Proactively replacing of the ISS assets, assessed with condition grades C4/C5 during the period 2017/18 – 2021/22.
- Reducing the risks associated with major ISS failure significantly at an estimated direct cost of $13.5M.
- Continuing inspection and maintenance activities (including testing) for ISS systems in compliance to relevant Australian Standards.
- Reactively replacing assets which during inspections and maintenance activities are identified as defective.

Condition, age and site risk data have been used to quantify the risks associated with the ISS assets fleet. A risk based replacement program greatly reduces exposure to significant financial and regulatory risks associated with a failing ISS asset (during security threat) to demonstrate an appropriate level of due diligence. This option reduces potentially significant health and safety and financial liabilities by replacing non-compliant assets which, following a risk assessment, have been deemed economically justified for replacement.

Choosing option 2 ensures that risks associated with ISS assets and age based degradation are addressed in the most economic manner. In addition risks associated with the failure of ISS assets are reduced which is especially important considering the possible health and safety consequence associated with any major security threat incident. Implementation of a risk based replacement program will maintain the improving levels of performance and reliability associated with the ISS assets fleet.

This option is recommended as it addresses all of the key business drivers listed in the Program Drivers section.

6.3 Option 3 – Age based replacement program

Implementing an age based replacement program and same standard upgrade program involves:

- Proactively replacing the ISS assets which have exceeded the average regulatory life of 40 years [C.I.C] and 12 – 15 years (for [C.I.C] and other similar assets).
- Upgrade most of the sites with same standards irrespective of risk assessments.
- Reducing the risks associated with major ISS failure significantly at an estimated direct cost of $18M.
- Continuing the inspection and maintenance activities for ISS assets.
- Reactively replacing ISS assets which during inspections and maintenance activities are identified as defective.

This option also addresses most of the key business drivers listed in the Program Drivers section but with significant extra cost in comparison to option 2 – the recommended option.

An age based replacement program reduces exposure to significant financial and regulatory risks associated with failing ISS asset to demonstrate an appropriate level of risk reduction. This option reduces potentially significant health and safety and financial liabilities by replacing ISS which are above the mean age of ISS assets. Also this option requires significant expenditure to raise the security measures level to the same standard at all sites.

Although this option also addresses most of the business drivers it requires approximately 66% more capex than the recommended option. Therefore, this option does not demonstrate efficiency and due diligence and hence is not recommended.

7 Financial Analysis

Each option has been financially analysed using an NPV model. Option 2 which is the condition/ risk based replacement option achieves the greatest amount of benefit for the lowest capital cost when compared to option 1 and 3. These benefits are based on significant risk reduction (95%) achieved through targeted replacement of ISS assets containing the high risk of major failure or installed on sites assessed with appropriate risk level. Although option 3 provides the maximum net present value but requires significantly higher capital expenditure (additional 50%).

The condition / risk based replacement option displays the lowest present value cost of $19.9M and the positive net present value as per Table 5.

Economic Analysis of Options ($'000s)	PV Capital Cost	PV Opex Costs	PV Community Benefits	PV Proceeds From Sales	Total PV Cost	NPV including Reg Return
Do Nothing	-	(7,581)	(22,678)	-	(30,260)	**-**
Upgrade/ replace security fencing, condition/risk based	(14,497)	(1,346)	(4,026)	-	(19,869)	**1,012**
Upgrade/ replace security fencing, aged/ same standard base	(20,629)	(695)	(2,080)	-	(23,405)	**2,183**
	-	-	-	-	-	**-**
	-	-	-	-	-	**-**

All figures are in $000's unless otherwise stated.
(nominal and discounted)

Table 5 – NPV Results – Security Fencing and Gates

8 Recommended Action

The risk based replacement program, Option 2, is recommended.

The proposed work program will target completion of upgrade works at RL1 sites along with risk and condition based upgrade work on most of the RL2 sites and some of the RL3 sites by 2020 and as per Table 6 below.

Description of Work	Number of Sites	Risk Level	Unit Rate ($k)	Estimated Cost ($k)
[C.I.C]	[C.I.C]	RL1 (Critical infrastructure sites)	[C.I.C]	2,250
[C.I.C]	[C.I.C]	RL1 sites only	[C.I.C]	4,500
[C.I.C]	[C.I.C]	RL1 & RL2	[C.I.C]	250
[C.I.C]	[C.I.C]	RL2	[C.I.C]	5,200
[C.I.C]	[C.I.C]	RL3	[C.I.C]	1,000
[C.I.C]	[C.I.C]	RL1 and RL2	[C.I.C]	300
TOTAL				**$13,500**

Table 6 – Proposed work program with number of sites and estimated cost

9 Reference Documents

- AMS 10 - 63 Infrastructure Security.
- AusNet Services' Station Design Manual (SDM), Volume 5, Section 13 – Civil design, Security fencing and signage.
- SPIRACS – AusNet Services' Incident Response and Contingency System:
    - Volume 1 – Administration Manual.
    - Volume 2 – Business Continuity Policy & Guideline.
    - Volume 3 – Crisis Management Policy & Guideline
    - Volume 4 – Emergency Management Policy and Guideline.
    - Volume 5 – Security Management System.
- AusNet Services' procedure RM 002, "Risk Assessment – Electricity and Gas Infrastructure Security".
- Guideline for the Prevention of Unauthorised Access to Electricity Infrastructure, 2005 ENA.
- AS/NZS 4360 (2004) – Risk Management.
- AS 1725 (1975) – Galvanised Rail-Less Chain Wire Security Fences and Gates.
- AS 2067 (1984) – Switchgear Assemblies and Ancillary Equipment for Alternating Voltages above 1 kV.
- AS/NZS 3000 (2003) – Electrical Installations.
- AS/NZS 3016 (2002) – Electrical Installations – Electric security fences.
- AS 2201 – Intruder Alarm Systems.
- AS 1319 (1994) – Safety Signs for the Occupational Environment.
- AS 4145 – Mechanical Locksets for doors in buildings.