Infrastructure Security

AMS – Electricity Distribution Network

PUBLIC

Document number	AMS 20-14
Issue number	5
Status	Approved
Approver	Paul Ascione
Date of approval	20/11/2019

ISSUE/AMENDMENT STATUS

Issue	Date	Description	Author	Approved
1	31/01/2009	Draft for discussion	D Postlethwaite	G Towns
2	20/02/2009	Update asset statistics section 4 Editorial Update risk assessments	M Matotek J Kenyon D Postlethwaite	G Towns
3	25/11/2009	Editorial & update schedule of medium & lower risk installations	D Postlethwaite	G Towns
4	2/12/2014	Editorial and update zone substation risk assessments	D Postlethwaite	J Bridge
5	20/11/2019	Editorial and updated sections to reflect current condition and quantities of assets.	F Lirios	P Ascione

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 Network Assets, Regulated Energy Services Division of AusNet Services. Please contact the indicated owner of the document with any inquiries.

AusNet Services
Level 31, 2 Southbank Boulevard
Melbourne Victoria 3006
Ph: (03) 9695 6000

Table of Contents

1 Executive Summary

This document is part of the suite of Asset Management Strategies relating to AusNet Services' electricity distribution network. Its purpose is to identify the issues, analyse options and define the strategy to maintain network reliability, safety and security through effective and efficient management of the physical security of network infrastructure.

Commonwealth and state governments have imposed legal responsibility on both the owners and operators of critical infrastructure – such as gas and electricity installations – to take all necessary preventative security measures to ensure continuity of supply. This strategy focuses on security enhancements for zone substations, ground-mounted kiosks, voltage regulators, substations and indoor substations, forming part of AusNet Services' electricity distribution network in the state of Victoria.

The main security threats to AusNet Services' electricity distribution network are:

- Safety – of untrained persons in the vicinity of energy-containing equipment.
- Malicious – motivated by revenge, fame, association or challenge.
- Criminal – profit driven; includes theft, fraud, sabotage or extortion.
- Terrorism – threat or use of force to influence government or public through fear or intimidation.[1]

1.1 Risk

The Infrastructure Security Risk Assessment Tool (ISRAT) is used to assess physical security risks to AusNet Services' installations and the electrical energy they transmit. This strategy is informed by site-specific risk assessments of major sites and generic assessments for the multiplicity of less significant installations.

1.2 Principles

AusNet Services' physical security control measures are founded on the following principles:

- Consistent risk identification and quantification.
- Defence in depth – increasing the number and sophistication of control measures commensurate with the degree of intrusion risk.
- Deterrence – measures to deflect would-be intruders towards other targets.
- Delay – measures to increase the time and effort required to successfully intrude.
- Detection – measures to promptly and reliably detect intrusion.
- Response – measures to promptly and appropriately deal with intruders and associated consequences.
- Contingency planning – measures to promptly recover service and minimise societal impact.

[1] A 'terrorist act' is an act or threat intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public; causing serious harm to people or property, creating a serious risk of health and safety to the public, disrupting trade, critical infrastructure or electronic systems – Criminal Code Act 1995 [Commonwealth].

1.3 Strategies

Strategies for the management of infrastructure physical security are contained in Section 7.11 of this document. The strategies cover:

- Zone substations;
- Voltage regulators and ground-type substations;
- Kiosk substations;
- Indoor substations; and
- Cable distribution cabinets.

2 Introduction

The Commonwealth and State governments have imposed legal responsibility on both the owners and operators of critical infrastructure, such as gas and electricity installations, to take all necessary preventative security measures to ensure continuity of supply. Owners and operators are expected to clearly recognise their responsibilities in safeguarding their installations as far as possible and to develop robust contingency plans to restore their services following a calamitous event (whether natural or man-made).

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 – to ensure the continued provision of supply.

The Electricity Safety Act requires AusNet Services to *design, construct, operate, maintain and decommission its supply network to minimise, as far as is practicable, the hazards and risks to the safety of any person arising from the supply network*.[2] What is considered "practicable" is determined by regard to:

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

AusNet Services is also required to meet the requirements of clause 3.1 (b) of the Electricity Distribution Code to:

(b) develop and implement plans for the acquisition, creation, maintenance, operation, refurbishment, repair and disposal of its distribution system assets and plans for the establishment and augmentation of transmission connections:
- *to comply with the laws and other performance obligations which apply to the provision of distribution services including those contained in this Code;*
- *to minimise the risks associated with the failure or reduced performance of assets; and*
- *in a way which minimises costs to customers taking into account distribution losses;*

Clause 6.5.7 of the National Electricity Rules requires AusNet Services to propose capital expenditures necessary to:

- *meet or manage the expected demand for standard control services over that period;*
- *comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;*
- *maintain the quality, reliability and security of supply of standard control services; and*

[2] Electricity Safety Act 1998, section 98(a).
[3] Electricity Safety Act 1998, section 3.

- *maintain the reliability, safety and security of the distribution system through the supply of standard control services.*

3 Objective

This strategy outlines security enhancements for AusNet Services' electricity distribution network in accordance with the aims and objectives outlined in SPIRACS[4], reproduced below for convenience.

> "Security management involves the protection of AusNet Services assets (infrastructure, people, information) from natural or deliberate threats. Credible threats and vulnerabilities shall be identified and mitigated; robust security controls introduced; and contingency plans developed and maintained to minimise the effects of security incidents, should they occur.
>
> An effective security management capability is necessary to minimise risks from security threats, and ensure compliance with regulatory and contractual obligations. The SPIRACS Corporate Security Policy establishes the requirement for a security management capability in AusNet Services, and specifically defines the policy in which potential or actual security incidents are to be effectively identified and managed".

The objectives of security management in AusNet Services are to:

- Minimise exposures to credible security threats
- Ensure that only authorised and appropriately trained personnel have access to assets
- Prevent unauthorised disclosure/access/loss/damage of corporate assets
- Prevent loss of asset functionality for the community, clients and customers
- Identify and respond to security incidents
- Minimise the impact of security incidents.

4 Scope

This document includes Strategies for the management of infrastructure physical security associated with the AusNet Services electricity distribution network in eastern Victoria. The scope of infrastructure covered by this document includes:

- Zone substations
- Voltage regulators and ground-type substations
- Kiosk substations
- Indoor substations
- Cable distribution cabinets
- Pole mounted installations
- Tower mounted installations
- Underground cables.

This document does not include information technology security strategies: please refer to the Information and Communication Technology Strategy[5] for information on this topic.

[4] SPIRACS – AusNet Services Incident Response and Contingency System.

[5] Information and Communication Technology Strategy CY2016 - CY 2020 Electricity Distribution Network, AusNet Services 2014

5 Asset Summary

AusNet Services has approximately 4,400 unmanned ground-mounted electricity installations where specific measures are required to control possible access to electrical conductors by unauthorised persons. These installations include zone substations, line voltage regulators, and ground-type, kiosk and indoor distribution substations.

An additional 97,300 cable distribution cabinets containing low voltage (LV) cable joints and switchgear exist in the form of public lighting columns and LV paralleling pillars. These installations are found in all public places, including commercial precincts, industrial subdivisions and residential subdivisions.

There are about 400,000 poles supporting high voltage (HV), medium voltage (MV) and LV conductors in the AusNet Services electricity distribution network. Poles rely heavily on a smooth surface without hand and foot holds for security against access to electricity conductors. AusNet Services also uses more than 11,000 km of HV, MV and LV underground cables in its distribution network. Underground cables rely on depth of burial, mechanical protection, marker tape and signage for security against access to electricity conductors.

Prior to 2006, these installations were designed and maintained to the security standards outlined in AS 2067[6] and ESAA guidelines[7] for design and maintenance of overhead lines. Since 2006 installations have been designed to the Energy Networks Association's (ENA's) national guidelines[8] and since 2010 designs have referenced AS/NZS 7000 for the design of overhead electrical lines[9].

5.1 Zone Substations

AusNet Services owns and operates 65 zone substations located in neighbourhoods ranging from remote rural to urban industrial and growing urban residential subdivisions. There are four basic types each supplying from 5,000 to 25,000 customers:

- Fully outdoor
- Semi-indoor
- Fully indoor
- Modular.

5.1.1 Fully Outdoor Zone Substations

In the eastern part of Victoria, 35 zone substations have air-insulated outdoor HV switchyards. Found in all types of neighbourhoods, the primary security feature is a 2.5 m high chain wire mesh fence, fitted in many cases with a barbed wire or barbed tape anti-climbing feature.

Large power transformers, located within the switchyard usually have exposed HV connections atop the transformer at heights exceeding 3 m. Transformer designs do not include any climbing aids; however, structural bracing and equipment mounting brackets provide sufficient hand and foothold for agile persons.

Switchgear is predominantly of the air-insulated type with exposed HV conductors located upon supporting structures at heights exceeding 2.8 m. Supporting structures for HV switchgear range from the relatively easy to climb 'lattice' style to the relatively difficult to climb 'portal' design.

Freestanding control rooms containing protection relays, control equipment and instrumentation, including SCADA terminals and communication equipment, are located within the switchyard. Some older control rooms contain exposed LV AC terminals and LV DC busbars mounted atop and at the rear of equipment-mounting panels at heights of 1.5 m to 2 m.

[6] Australian Standard AS/NZS 2067 HV Installations.
[7] Guidelines for the Design and Maintenance of Overhead Lines C(b) 1 – 2003, Electricity Supply Association of Australia.
[8] National Guidelines for the Prevention of Unauthorised Access to Electricity Infrastructure, ENA Doc 015–2006
[9] Australian Standard AS/NZS 7000.

Padlocks and locks control access to all gates and external doors. Key issue is restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are displayed at all sites. Intruder-detection systems, smoke detectors and SCADA alarms are common. Remote control of switchyard security lighting is fitted at some sites.

Landscaping has improved the visual aesthetics at many sites and, in some cases, reduced the natural surveillance of the switchyards and control room buildings.

5.1.2 Semi-Indoor Zone Substations

There are 25 of this type of zone substation found in all neighbourhoods. They feature an outdoor 66 kV switchyard secured by chain wire mesh security fencing and gates of a similar standard to that of fully outdoor designs.

Locked doors secure access to the brick sound enclosures containing the large power transformers in the switchyard. No climbing aids are provided and there are few equipment-mounting brackets to provide hand and foot holds for climbing the 4 m to the top of the sound enclosures where exposed HV connections are situated.

Exposed 66 kV conductors and air-insulated switchgear are supported on relatively difficult to scale ‘portal’ type structures.

The MV switchgear is of a fully insulated metal-clad type located in a single room within a locked brick building. This building also forms part of the external security fencing for the site. Protection, control and instrumentation equipment and batteries are also located within the building. There are no exposed conductors within the building.

Similar access controls, signage, detection systems and remote alarms relating to fully outdoor zone substations also apply to semi-indoor installations.

5.1.3 Indoor Zone Substations

AusNet Services currently has one indoor zone substation, the Hampton Park Zone Substation. All HV and MV switchgear is contained within a single brick building that has few access doors and fixed windows minimising unauthorised entry.

66kV air-insulated switchgear and 22 kV metal-clad switchgear is enclosed within locked switch rooms and the transformers are contained within brick sound enclosures. Only the 66 kV conductors and switchgear are air-insulated; all other auxiliary power and control system conductors are fully insulated. Some PVC coated chain wire mesh security fencing controls access to MV capacitor banks.

Padlocks and locks control access to all gates and doors. Key issue is restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are installed at all sites. Intruder detection systems and SCADA alarms are fitted.

Landscaping has been employed to improve the visual aesthetics but has no impact on the natural surveillance of the building.

5.1.4 Modular Zone Substations

Modular zone substations are becoming the contemporary design standard. They are generally located in growth corridors adjacent to urban residential neighbourhoods. They feature an outdoor 66 kV switchyard secured by chain wire mesh security fencing and gates of a similar standard to that of fully outdoor designs.

Large power transformers located within the switchyard usually have exposed HV connections atop the transformer at heights exceeding 3 m. The design does not include any climbing aids; however, structural bracing and equipment-mounting brackets provide sufficient hand and foot holds for agile persons. Exposed 66 kV conductors and air-insulated switchgear are supported on relatively difficult to scale ‘portal’ type structures.

MV switchgear is of a fully insulated metal-clad type located in a secure steel-clad modular re-locatable building within the external security fence. Insulated conductors, protection, control and instrumentation equipment, auxiliary power and batteries are located within similar buildings.

Similar access controls, signage, detection systems and remote alarms relating to fully outdoor zone substations also apply to package zone substation installations.

5.1.5 Security Fences

The primary security measure at most zone substations is an intruder-resistant chain wire mesh fence located on the property boundary or around the HV switchyard. Approximately 23 km of security fencing encloses approximately 71 sites to resist unauthorised entry into HV switchyards and buildings.

The majority of security fences utilise a chain-wire mesh panel mounted on galvanised posts topped with multiple strands of barbed wire or barbed tape. Other types of fencing panels used are timber palings, metallic panels, PVC coated wire mesh and welded mesh panels. As per AS2067[10] the current requirement for a HV enclosure fencing installation to minimize the risk of unauthorized access through easy climbing or excavation is as following.

- Minimum height 2.5 m.
- Barbed wire (or similar) topping with at least four strands.
- Maximum gap of bottom wire with ground 50 mm.

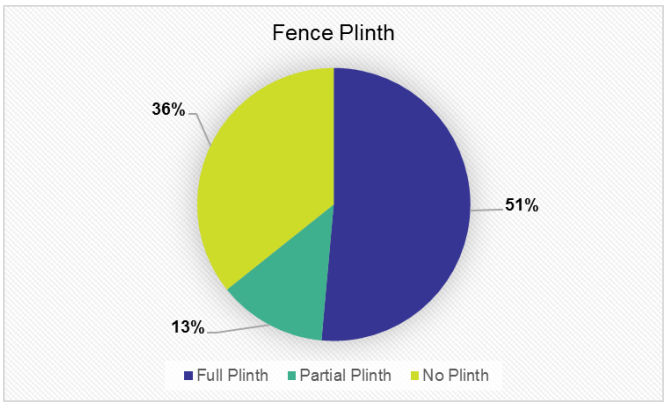
In addition to the minimum standard requirements AusNet Services periodically reassesses security risks using a purpose built Infrastructure Security Risk Assessment Tool (ISRAT).

In accordance with the assessed security risks improved security fencing which includes the following features is being implemented

- Concrete plinth to resist burrowing or tunnelling
- Top and bottom metallic rails to resist loosening of wire mesh
- Razor wire toppings in concertina configuration to increase the overall effective height to minimum 2.9 m to resist climbing

In addition to condition based treatment, AusNet Services also plans to increase the security controls at high-risk sites[11]. Measures to increase security above the existing standard include electrified fences; weldmesh or palisade fence construction; electronic access to buildings and stations; intruder detection in stations and buildings and in conjunction with electric fencing; remote-control lighting, motion detection recording and cameras; padlocks on outdoor electrical control boxes. Installation of remote-control lighting and cameras will require sufficient communications infrastructure available at the site.

Figure1 below shows that a full plinth to deter or restrict access and to structurally reinforce the fence is in place at 51% of security fences. The remainder of security fences have no footing or plinth (36%) to limit under-fence access or a partial plinth (13%).



[10]AS 2067: Substation and high voltage installation exceeding 1 kV.
[11] See Appendix X for the list of high-list sites as determined by the Security Department of AusNet Service

Figure 1 – Footing Plinths under Security Fences

Intruder-resistant fences have a topping of barbed wire or barbed tape (razor tape) to provide a climbing deterrent. Although the industry now considers this ancillary item to be a weak climbing deterrent, security fences of zone substations need to be progressively fitted with barbed tape and the effective fence height increased to 2.7 m.

At some sites, adjacent buildings or trees compromise the overall height of the security fence so a minimum one-metre clearance is required to maximise the effectiveness of the security fence. Where a clear zone cannot be established the re-alignment of the fence or additional fence height may be required.

5.1.5.1. Security Fence Condition Assessment

Each zone substation was assessed based on lacking additional safety measures (ASM) and condition of existing fencing against the effectiveness of fencing to deter intrusions.

Table 1 demonstrates the condition score and description.

Table 1 – Fencing condition assessment

Condition Assessment Score	Fencing Condition Description	Remaining Service Life (Years)
C1	New fences, all ASM installed and compliant to current standard AS2067	50
C2	Chain wire mesh with plinth and topping, top and bottom rails, no deterioration signs, all of the ASM installed	40
C3	Topping with additional height, lacking plinth or topping, good condition mesh/ timber, no deterioration sign, lacking 1 or 2 ASM	20 – 40
C4	Barbed wire but no plinth, no top and bottom rails, mixed condition, rusting signs, non-standard height, lacking up to 3 ASM	5 – 20
C5	No topping, no plinth, no top and bottom rails, on most of the fencing, ageing signs (rusting or cracking), non-compliant heights (< 2.5m) and lacking all or up to 4 ASM	Less than 5

As shown in Figure 2, the condition of security fences on zone substations have improved due to the infrastructure security and station rebuild projects in the current period. More than 50% of AusNet Services' substations are fenced with PVC coated wire mesh; razor tape and plinth and top and bottom rails. These are in accordance with the current standard AS2067.

Approximately 25% of the stations' fences are not up to the current standards without any topping, plinth and top and bottom rails, in most of the cases exhibiting potential risk of compromised security due to lack of additional security measures.

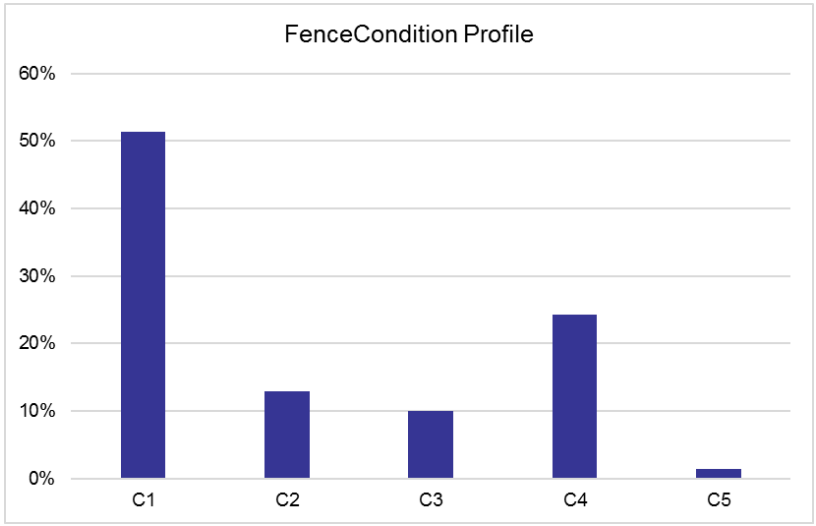


Figure 2 – Condition profile of fencing assets

Only one percent of the stations have a fence condition of "Very Poor" (C5). This site will be improved by a station rebuild project in the coming EDPR period.

5.1.6 Control Buildings

Freestanding control rooms containing protection relays, equipment controls and SCADA terminals are located within the switchyard of most zone substations. Unauthorised access and fires in control buildings are significant threats to supply reliability. The following figures summarise the intruder resistance and fire resistance of existing control buildings provided by the building and roofing materials.

As seen in Figure 3 below, intruder-resistant steel-sheet roofing can be found on a majority of control room buildings. The remainder consist of asbestos containing material (ACM) sheeting and cement or terracotta roof tiles, which, whilst fire resistant, provide limited security benefit.

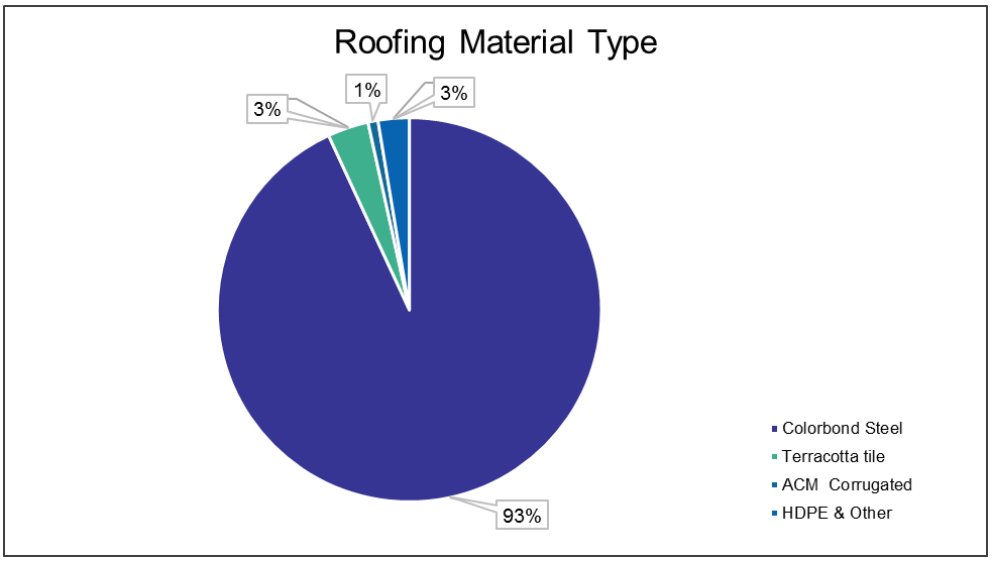


Figure 3 – Roofing on Control Buildings

Fire and intruder-resistant brick, concrete and steel-sheeting walls comprise 95% of control room buildings, as illustrated in Figure 4. Brick and concrete walls provide the maximum mechanical strength and projectile resistance. The remaining 5% of external walls are comprised of weatherboards, ACM sheeting and Hardie Planks. These provide minimal security benefit. Weatherboards (wood boards) also have a low fire rating.

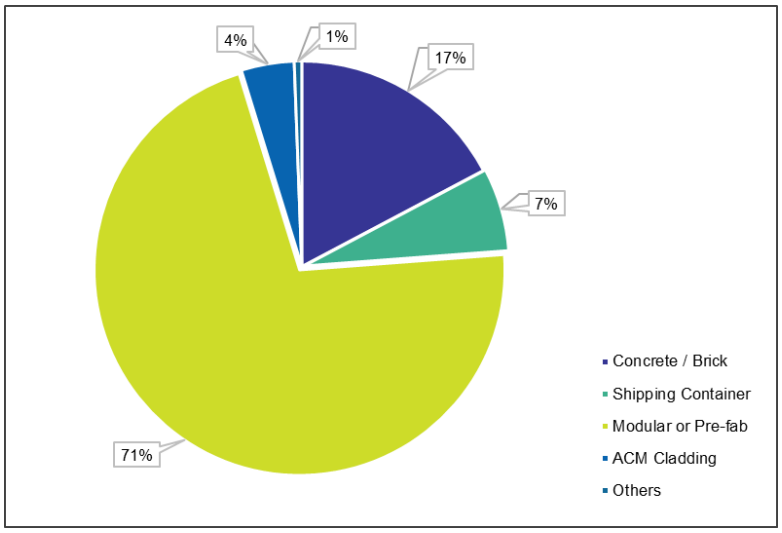


Figure 4 – External Walls on Control Buildings

Some control rooms have hollow core doors on external entrances with only cardboard waffle internal packing. These doors have a low fire rating and many also have a glass insert which further compromises their low mechanical strength. Approximately one third of control room external doors are made from steel, solid timber or solid timber with glass inserts and grilles which provide adequate security and fire ratings.

5.1.6.1. Buildings Condition Assessment

Refer to AMS 20 - 55 Civil Infrastructure for Buildings Condition Assessment

5.2 Voltage Regulators

AusNet Services has 89-line MV voltage regulators sites, of a traditional design configuration, to maintain the steady state voltages of lines supplying from 2,000 to 5,000 customers. Found on road reserves in rural areas the primary security feature is a 2.5 m chain wire mesh fence, fitted in some cases with a barbed wire anti-climbing feature.

The voltage regulating transformers are located within a small switchyard with covered MV connections atop the transformer at heights exceeding 3 m. The design does not include any climbing aids; however, structural bracing and equipment-mounting brackets do provide sufficient hand and foot holds for agile persons.

The limited switchgear in these installations is mounted on a pole at heights exceeding 4m. However, it is possible to climb to the exposed conductors of this switchgear via the transformer tank.

Padlocks and locks control access to all gates. Key issue is restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are installed at all sites. Intruder-detection systems, alarms and remote control of yard/security lighting are not installed. Regrowth of native vegetation can reduce the natural surveillance of these switchyards.

5.3 Ground-Type Substations

There are 550 of these traditional design configuration distribution substations located primarily on privately owned property in urban industrial estates. Supplying from 5 to 50 customers each, the only security feature is a 2.5 m high chain wire mesh fence fitted, in some cases, with a barbed wire anti-climbing feature.

Large transformers are located within these small switchyards with covered HV connections atop the transformer at heights exceeding 3m. Although no climbing aids are provided in the design, structural bracing and equipment-mounting brackets do provide sufficient hand and foot holds for agile persons.

There is limited switchgear within these installations and it is mounted on a pole at heights exceeding 4m. However, it is possible to climb to the exposed conductors of this switchgear via the transformer tank. Some installations contain exposed LV busbars and switchgear mounted on simple structures at heights of 2.5m.

Some sites benefit from the security measures employed by the owner of the private property concerned; however these measures are usually negated during business hours.

Padlocks and locks control access to all gates. Key issue has been restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are installed at all sites. Intruder-detection systems, alarms and remote control of yard/security lighting are not employed.

Landscaping to improve the visual aesthetics is unusual, but material storage on adjacent land can reduce the natural surveillance of these switchyards.

5.4 Kiosk Substations

AusNet Services employs more than 3,356 kiosks featuring a weatherproof enclosure containing a transformer, MV and LV switchgear, and doors to facilitate operation and maintenance from outside the enclosure. Kiosks are usually located on publicly accessible properties in urban residential or commercial neighbourhoods. They each supply from 100 to 500 customers.

Their construction; using High Density Polyethylene (HDPE) glass-reinforced fibre and painted or galvanised sheet metal provides the degree of penetration protection (IP34) in accordance with AS 1939.

All live switchgear, including busbars, connections, circuit breakers, isolators and transformers provide an IP2x degree of protection in accordance with AS 1939. Doors and covers facilitating access to operating interfaces are locked.

Key issue has been restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are installed at all sites. Intruder-detection systems, alarms and remote control of yard/security lighting are not employed.

Landscaping to improve the visual aesthetics is common, sometimes reducing the natural surveillance of sites.

5.5 Indoor Substations

In AusNet Services' Victorian electricity distribution network there are 550 distribution substations featuring the complete enclosure of all MV and LV switchgear within a privately owned building. Located within urban commercial environments, the windowless single room substation has a pedestrian door and a pair of ventilated equipment access doors. They supply from 5 to 500 customers.

MV and LV switchgear is usually of the fully insulated type, although a few older installations feature air-insulated switchgear and exposed conductors mounted on internal walls or the ceiling at heights in excess of 2.4 m. Transformers and LV switchgear are contained within the same room, with some exposed electrical terminations. In a limited number of installations, exposed LV busbars are mounted on the walls.

Padlocks and locks control access to all doors. Key issue has been restricted to trained personnel. Signs showing contact phone numbers and warning of HV equipment and of the dangers of unauthorised access are installed at all sites. Intruder-detection systems and alarms are not common and features such as closed circuit television (CCTV) and remote control of security lighting is unusual.

The location of these substations in loading bays, laneways and other unobtrusive sites often limits the degree of natural surveillance available to passers-by.

5.6 Cable Distribution Cabinets

5.6.1 Public Lighting Columns

AusNet Services manages in excess of 151,000 public lighting installations, most of which are mounted on solid timber and hollow concrete line poles. However, there are approximately 89,000 dedicated public lighting columns formed from hollow steel structures lighting major roads and residential subdivisions.

Within each column a switch and fuse panel protects the lantern and lamp. Whilst the cables and joints are fully insulated, traditionally the LV fuse terminals on the switch/fuse panel have been exposed. Access is facilitated by removing a panel, using a security tool available to authorised personnel. However, instances have occurred where determined persons have overcome this simple security feature.

5.6.2 LV Paralleling Pillars

An additional 8,300 LV pillars are found in residential subdivisions to facilitate the paralleling of LV underground circuits between adjacent kiosk substations. These pillars are protected by a removable fibreglass cover and secured by a stainless steel security tie and seal combination. There is limited warning signage on these pillars. Whilst the LV cables and terminations are fully insulated, the switch/fuse terminals have traditionally been exposed.

5.7 Pole-Mounted Installations

There are 45,730 small capacity transformers mounted on poles supplying customers in the eastern part of Victoria. There are more than 15,000 HV switches mounted on poles to control the flow of electrical current in the electricity network. In total there are approximately 400,000 timber and concrete poles supporting bare and insulated electrical conductors.

Access to the HV and LV electrical equipment on these poles is controlled by the following standard design features:

- Locating poles away from other structures and vegetation
- Installing hardwood and concrete poles with smooth external surfaces
- Mounting electrical equipment and controls at heights exceeding 3 m above ground level
- Mechanically protecting and electrically insulating equipment accessible from ground level
- Eliminating hand and foot holds on equipment accessible from ground level
- Installing signage warning of electrical hazards.

Where the above controls are not deemed adequate, anti-climb features such as barbed wire or barbed tape is added to minimise the risk of scaling the pole.

5.8 Tower-Mounted Installations

AusNet Services employs 481 galvanised steel towers to support several 66 kV sub-transmission circuits. These towers are of a lattice type construction; similar to those employed in the Victorian electricity transmission network and are located in transmission circuit easements within private property.

Access to easements is controlled by padlocked gates. Access to individual towers is controlled by an anti-climbing barrier of steel mesh and barbed wire mounted on each tower. This anti-climbing barrier is secured by a security padlock.

Keys for these security locks are only issued to staff and contractors who are formally trained and authorised to climb these towers. Keys are managed from a single register to ensure effective control.

5.9 Underground Cables

There is more than 2,170 km of HV underground cable and 10,800 km of LV underground cable supplying customers in the eastern part of Victoria. Underground cable is the standard medium for connecting up to 10,000 new residential customers each year in the urban growth corridors south-east and north of metropolitan Melbourne.

Access to these HV and LV underground cable is controlled by the following standard design features:

- Locating poles away from other underground assets such as telecommunication cables, water, sewerage and gas pipes
- Installing underground cables at depths exceeding 450 mm
- Mechanical protection such as conduits and nonconductive cover slabs
- Installing warning marker tapes above the cable or its mechanical protection
- Installing signage warning of electrical hazards where cables emerge from below ground.

Accurate records detailing the location of cables and the provision of information to authorised persons wishing to excavate in the vicinity are important factors in maintaining the physical security of underground cable systems.

6 Risk Management

6.1 Threats

Geographically dispersed in all neighbourhoods, unmanned installations in the electricity distribution network present diverse security challenges. With potential impacts on members of the public, the local community and on the commercial viability of network owners/operators, these security threats have been classified as:

- Safety – of untrained persons in the vicinity of energy containing equipment.
- Malicious – motivated by revenge, fame, association or challenge.
- Criminal – profit driven; includes theft, fraud, sabotage or extortion.
- Terrorism – use or threat of force or violence to influence government or public through fear or intimidation.

Figure 5 below illustrates the predominant threats for each type of installation.

	Safety	Malicious	Criminal	Terrorism
Zone Substations	Yes	Yes	Yes	Yes
Voltage Regulators	Yes	Yes	Yes	
Kiosk Substations	Yes	Yes		
Ground-Type Substations	Yes	Yes	Yes	
Indoor Substations	Yes	Yes	Yes	
Cable Distribution Cabinets	Yes	Yes		
Substations on Poles	Yes	Yes		
Switches on Poles	Yes	Yes		
Poles	Yes	Yes		
Underground Cables	Yes			

Figure 5 – Security Threats by Installation Type

6.2 Procedures

SPIRACS Volume 5 Part 2 'Security Management Framework' and Part 3 'Operational Security Policies, Standards & Procedures' contain information and references on the authorised policy and procedures to be employed when:

- Authorising employees and contractors to enter AusNet Services sites.
- Entering AusNet Services sites.
- Reporting unauthorised access events.
- Monitoring and responding to unauthorised access events.
- Inspecting, testing, maintaining and auditing physical security measures.
- Developing, exercising and maintaining contingency plans.

6.3 Risk Assessments

The 2017 version of the Infrastructure Security Risk Assessment Tool (ISRAT) has been used to assess physical security risks and control measures in ground-mounted installations forming part of AusNet Services electricity distribution network.

Infrastructure Security

ISRAT is a quantitative tool based on the principles in Energy Network Association's national guidelines and the risk assessment methodology in the international risk management standard ISO 31000.

ISRAT produces assessments of risk for safety, theft, unauthorised operation and terrorism threats. Risk assessments are undertaken:

- During planning and design of new sites.
- Following an unauthorised access event.
- Where major changes are made to existing sites where security may be compromised.
- When neighbouring land is re-zoned or its main use is significantly changed.
- Where a risk assessment has not been carried out for five years.

This strategy has been informed by site specific assessment of the security risks at each zone substation[12] and generic assessments for the multiplicity of smaller distribution installations.

6.3.1 Higher Risk Zone Substations

The following 16 zone substations are currently classified as higher security risk:
[C.I.C]

6.3.2 Medium Risk Zone Substations

The following 18 zone substations are currently classified as medium security risk:
[C.I.C]

6.3.3 Lower Risk Zone Substations

The following 34 zone substations are currently classified as lower security risk:
[C.I.C]

[12] ISRAT Zone Substation 2017.xlsx December 2017AusNet Services.

7 Control Measures

7.1 Principles

Controls limit the extent of, and define the response to, a breach of security. It is acknowledged that, with portable power tools widely available, it is impractical to prevent determined persons from gaining unauthorised access to every site. Nevertheless, AusNet Services employs a range of security controls to deter would-be intruders, to delay and detect unauthorised entry events and to promptly respond to and/or recover from the impact of such entry. Physical security control measures are founded on the following principles:

- Consistent risk identification and quantification.
- Defence in depth – increasing the number and sophistication of control measures commensurate with the degree of intrusion risk.
- Deterrence – measures to deflect would-be intruders towards other targets.
- Delay – measures to increase the time and effort required to successfully intrude.
- Detection – measures to promptly and reliably detect intrusion.
- Response – measures to promptly and appropriately deal with intruders and associated consequences.
- Contingency planning – measures to promptly recover service and minimise societal impact.

Sites are defined in a manner that discourages anti-social behaviour such as loitering, littering, graffiti and vandalism, which frequently precede unauthorised entry. Definition includes site delineation using boundary fences or natural barriers such as plants or rocks and extends to signs requesting that third parties report inappropriate behaviour.

Territorial reinforcement aims to deflect intruders toward softer targets through the use of obvious physical security measures such as lighting, fencing, re-enforced doors and window grilles and extends to prompt removal of graffiti and repair of vandalism and the use of electronic security warning signs. To deflect potential intrusion attempts, sites are maintained in a neat and tidy manner with vegetation regularly trimmed, grasses mown and litter removed.

The contents of sites are securely stored. Portable items of value are secured in areas not readily visible from the site exterior. Materials, vehicles and equipment are inventoried and stored in an orderly manner so that theft or attempted theft is obvious.

Natural surveillance involves surveillance zones through landscaping, where trees are pruned up and shrubs are trimmed down, to provide visibility of access points, site perimeter, buildings and equipment. This allows neighbours, staff or legitimate passers-by to scrutinise the activities of potential intruders. In particular, trees and shrubs are not established such that they mask visibility of the site perimeter or the switchyard interior.

7.2 Intruder Resistant Fencing

7.2.1 Principles

Intruder-resistant fencing is designed to exclude persons not equipped with tools and delay access by those equipped with tools from selected areas of infrastructure sites.

The foundations and structural supports of fencing are designed to resist the manual efforts of potential intruders. Fencing utilises robust materials such as brick, masonry, chain wire mesh, sheet metal, weldmesh or steel palisade, arranged so as to minimise the possibility of unauthorised persons penetrating, scaling or undermining the fence.

The location, construction and use of gates are designed to complement the function of intruder-resistant fences. Particular attention is required to ensure locking devices and gateposts minimise scaling of the gate or fence.

Where motor vehicles are assessed as credible risk, vehicular barriers such as [C.I.C] railings, concrete barriers, drainage ditches or earth mounds are incorporated in the overall fencing design.

Where space permits at sites assessed as a higher risk of unauthorised access, 'clearance zones' are established immediately adjacent to security fencing to minimise the threat of scaling by use of nearby aids such as vegetation or stored materials. If space is restricted, the total effective height of fencing is increased in proportion to the risk of scaling.

7.2.2 Declared Critical Sites

There are 13-sites that has been declared as Critical Sties under the Emergency Management Act of the Minister. These sites are included in the list given in section 6.3.1 and are planned to have swipe card entry into the station gates and buildings, as well as sensors and cameras to monitor activities and provide real-time detection.

7.2.3 Higher Risk Sites

Where assessment indicates higher risks of unauthorised access, intruder-resistant fences may consist of Type 2 – Pipe rail security fencing[13] or equivalent weldmesh security panels, palisade panels, brick or masonry walls of a minimum 2.4 m in height with a concrete or cement stabilised crushed rock footing or kerb and a barbed tape anti-climbing device in flat loop or concertina configuration to bring effective fence height to greater than 2.9 m.

Figure 6 below illustrates a security fence comprising weld mesh security panels, continuous concrete footing plinth and a short-barbed tape anti-climbing feature in concertina configuration suitable for higher security risk sites.

[13] Australian Standard AS 1725.1-2010 Chain link fabric fencing Part 1 Security fences and gates.

Figure 6 – Weldmesh Security Panel with Concrete Plinth and Barbed Tape

Where assessment indicates higher risks of unauthorised access; existing intruder-resistant fences can be enhanced with:

- An electronic access system.
- a micro phonic or vibration-based perimeter detectors.
- electric power fencing.

An electric power fence is located on the inside of the chain wire mesh panel. Its lowest wire is less than 150 mm above ground level and its upper wire is 2.9 m above ground level. In-riggers, out-riggers, barbed wire or barbed tape are not used in conjunction with an electric power fence. The electric power fence installation shown in Figure 7 includes intrusion alarm monitoring via SCADA.

Figure 7 – Electric Power Fence inside Chain Wire Mesh Fence

7.2.4 Medium Risk Sites

For sites assessed as a medium risk of unauthorised access, intruder resistant fencing may be constructed from chain wire mesh to the following standards:

- Type 2 - Pipe rail security fence to AS 1725.1-2010 Chain link fabric fencing Part 1 Security Fences and Gates.
- AS 2067:2008 Substations and high voltage installations exceeding 1 kV a.c.

The minimum height of fence panels is 2.4 m. Each fence panel shall not be more than 50 mm from the ground. Risers fitted with flat looped short-barbed tape provide an anti-climbing feature to a minimum effective fence height of 2.9 m. A combination of fence footings, kerbings or rails is used to restrict the ability of intruders to pass under the fence as shown in Figure 8 below.

Figure 8 – Pipe rail security fence to AS 1725.1

7.2.5 Lower Risk Sites

For sites assessed as a lower risk of unauthorised access, intruder resistant fencing to the following standards:

- Type 1 – Rail-less security fencing consistent with AS 1725.1-2010 Chain link fabric fencing Part 1 Security Fences and Gates.
- AS 2067:2008 Substations and high voltage installations exceeding 1 kV A.C.

The minimum height of fence panel is 2.1 m. The fence panel shall not be more than 50 mm from the ground. Risers or in riggers or out riggers fitted with multiple strands of barbed wire or a flat looped short-barbed tape anti-climbing feature to a minimum total height of 2.5 m as shown in Figure 9 below.

Figure 9 – Type 1 Rail-less security fence to AS 1725.1

7.3 Electronic Access Controls

Commensurate with a high level of assessed risk, electronic access control systems may be installed on pedestrian gates in the security fence or on external building doors leading to control and relay rooms. Electronic proximity cards permit entry to authorised employees and contractors via an interface similar to that illustrated in Figure 10 below.

Figure 10 – Electronic Access Control, User Interface

Access controls are capable of giving specific permission to individual persons on a site-by-site basis and can be used to restrict access to certain times or under certain conditions. The electronic access control system provides access history and alarm signals to the network operation centre when unauthorised access is attempted.

7.4 Buildings

Where buildings form part of the security perimeter of a site, they are designed to provide intruder resistance equivalent to that of the security fence. Where a building is fully enclosed within the security perimeter, a risk assessment assists in determining appropriate security measures.

Buildings are constructed of robust materials such as brick, masonry or sheet metal cladding, arranged so as to minimise the possibility of unauthorised persons penetrating, scaling or undermining the building. Roofs are made of steel sheeting securely fastened to prevent removal. Building designs feature minimal climbing aids such as down-pipes, windowsills and architectural features as illustrated in Figure 11 below.

Figure 11 – Intrusion Resistant Building

External doors in new and re-furbished installations are solid core timber or steel faced and bear against a steel frame fixed to adjoining walls. Door strength and fire rating are not compromised by vents or windows; hardware has concealed fixings and tamper-resistant hinges. External openings to underfloor spaces or ceiling spaces, such as cable access or pulling holes, windows, vents and skylights, at higher risk sites are secured with security grilles similar to those shown in the following Figure 12 below.

Figure 12 – Security Grilles over Existing Windows

7.5 Locks and Keys

Entry points at zone substations, distribution substations and communication sites that are not fitted with electronic access controls are secured with locksets and padlocks complying with AS 4145 – Mechanical Locksets for doors in buildings.

Keys are only issued to staff, contractors and agents who are formally trained and authorised to enter specific areas and sites. The issue, receipt and return of keys is managed from a single register and audited to ensure effective control.

Periodic replacement of locks and padlocks and re-issue of new keys to authorised persons is the most economic and pragmatic technique for managing lost, misplaced and stolen mechanical keys.

7.6 Signage

Installations are signed at entrance points and at regular intervals along the site boundary or security perimeter to achieve the following objectives:

- Display ownership of the property
- Mandate controlled access by authorised persons
- Provide contact phone numbers for emergencies, to report suspicious activity or seek return of lost property such as sports balls
- Warn of occupational hazards such as HV or extreme operating pressures
- Warn of the use of electronic surveillance and alarms, and the use of security measures such as barbed tape, electric power fencing and Data Dot marking.

Signs are placed where they are noticeable and the message is clearly visible. They are secured in a tamper-resistant manner in locations that do not compromise other occupational hazard signs. As per AS 1319, where electric power fencing, cameras or other surveillance tools are used, this is also signed along the perimeter.

7.7 Intrusion Detection

Commensurate with the level of assessed security risk, intrusion detectors are installed within selected spaces and openings in zone substations to detect and verify unauthorised access attempts.

The Network Operation Centre undertakes alarm monitoring and response management in accordance with AS 2201 and AS 4421 and procedures established in SPIRACS Volume 5 Part 2 Security Management Framework.

7.7.1 Site Perimeter

Microphonic or vibration-based perimeter detectors such as the [C.I.C] systems[14] may be installed on existing higher risk security fences as stand-alone systems or in conjunction with electric power fencing to detect attempts to penetrate, scale or undermine the security fence.

7.7.2 Site Interior

CCTV cameras may be installed to monitor access points, switchyards and buildings within selected high security risk sites. Options include permanent installations to monitor sustained security risks and temporary installations to monitor time-specific risks such as construction projects.

CCTV cameras can operate in conjunction with intrusion detectors, security lighting and remote operation to detect, verify and assist the response to unauthorised access attempts. Access to the images from the cameras is restricted to authorised personnel, as per AusNet Services policy 'Use of Surveillance Camera Equipment'.

[14] SENSTAR products.

7.7.3 Building Interior

Motion detectors are used in switch rooms, relay rooms and battery rooms within selected sites to detect unauthorised access. Commensurate with the level of assessed security risk, motion activated CCTV cameras may also be employed within zone substation buildings.

7.8 Lighting

Security for zone substations incorporates lighting designed to:

- Deter nearby anti-social behaviour
- Deter unauthorised access
- Facilitate identification of unauthorised access activity
- Assist staff and security personnel in responding to network events and unauthorised access attempts.

The standard and extent of lighting and the sophistication of lighting controls is matched to the assessed risk of unauthorised access. The entrances and the pathways within sites are capable of illumination to ensure night visibility for staff. Switchyards are lit to levels that enable operational activities to be performed. Remote activation of switchyard and building lighting from the network control room facilitates the response of security contractors to unauthorised access alarms.

Where credible security risks have been assessed, supplementary lighting will enable CCTV monitoring and facilitate response to unauthorised access attempts.

When planning the installation or augmentation of operational and security lighting the following factors should be considered:

- Manual, remote, time-switch or motion-sensing activation.
- Restrike time for high-intensity discharge lamps.
- Light pollution on neighbouring properties and the night sky.

7.9 Patrols and Monitoring

Security guards are contracted to monitor equipment and materials at construction sites and to respond to security events at operational sites. The extent and sophistication of security monitoring is adjusted according to prevailing risk levels.

7.10 Inspection Testing Maintenance and Auditing

Commensurate with the assessed level of security risks:

- Sites are inspected for indications of unauthorised entry.
- Control measures are inspected and tested to ensure functionality.

Inspections are carried out at intervals defined in the Standard Maintenance Instruction on-site inspections. At times of heightened threat classification or alert, inspections may be required at more frequent intervals. Inspections include specific checks for indications of unauthorised entry to each site. Inspections also assess the condition of any installed controls, especially fences, gates and building access points for general wear.

Controls deemed to be in poor condition are reported and remedied within the timeframes specified by SPIRACS.

Periodic audits are conducted to confirm the integrity of the overall security system in accordance with the provisions established in SPIRACS. Audit scopes include:

- Recent security system performance.
- Compliance with established policy, procedures and standards.
- Relevancy and adequacy of established policy, procedures and standards.

7.11 Contingency Plans

A network contingency plan is prepared for the electricity distribution network each year. Whilst this plan is focussed on the recovery of service following plant failure or a natural disaster such as flood or fire; elements of this plan are suitable for response to unauthorised access events in zone substations. In conjunction with SPIRACS these plans enable rapid deployment of skilled people, specialised construction equipment and spare equipment to safely restore electricity supplies.

For those sites assessed as a particularly high security risk; specific contingency plans to manage the recovery of service provision following an unauthorised access event may be prepared.

8 Strategies

8.1 Zone Substations

8.1.1 Declared Critical Zone Substations

In a specific security improvement program by 2026, undertake the following at [C.I.C]:

- Replace poor condition fence with 358 Mesh fence
- Introduce swipe card entry into switchyard and buildings, install sensors and cameras to provide real-time detection of intruders.

8.1.2 New Zone Substations

New zone substations shall incorporate the following security measures:

- Site hazard warning signs and security signage.
- Intruder resistant security fence of Type 2 - Pipe rail security fencing[15] or equivalent weldmesh security panels or palisade panels or brick or masonry walls of a minimum 2.5 m in height with a concrete footing plinth and a barbed tape anti-climbing device to an effective height of 2.9 m.
- Buildings with projectile-resistant walls, security and fire-rated doors and window grills.
- SCADA monitored motion detectors within relay rooms and switch rooms.
- SCADA control of switchyard and building lighting.
- Restricted keyed pad locks or swipe entry card on security fence gates and building exterior door locks.
- Restricted keyed locks on the operating controls of all electrical equipment.
- Data Dot marking of exposed earthing conductors.

8.1.3 High Risk Zone Substations

In a specific security improvement program at [C.I.C] by 2026:

- Install new switchyard lighting and sensors

8.1.4 Medium Risk Zone Substations

In conjunction with network augmentation and asset replacement projects at [C.I.C] by 2026:

- Review and update hazard warning signs and security signage.
- Review Data Dot marking of exposed earthing conductors.
- Install footing plinths under existing security fences.
- Convert existing security fences to Type 2 - Pipe rail security fencing.
- Install razor tape on risers on existing intruder-resistant security fence.
- Harden the exterior of control/relay buildings with projectile-resistant walls, security and fire-rated doors and window grills.
- SCADA monitoring of motion detectors within relay and switch rooms.
- Install SCADA controls for switchyard and building lighting.
- Lock operating controls on electrical equipment.
- Incorporate security in generic contingency plans including spare equipment holdings.

[15] Australian Standard AS 1725.1-2010 Chain link fabric fencing Part 1 Security fences and gates.

In a specific security improvement program at [C.I.C] by 2026:

- Install new switchyard lighting and sensors

8.1.5 Low Risk Zone Substations

In specific security improvement projects at [C.I.C] by 2026:

- Install risers and flat looped barbed tape anti-climb measures on existing security fences.
- Install SCADA controls for switchyard and building lighting.

8.2 Voltage Regulators and Ground Type Substations

In conjunction with network augmentation and asset replacement projects:

- Review hazard warning signs and security signage.
- Install footing plinths under existing security fences.
- Convert security fences to Type 2 - Pipe rail security fencing.
- Install razor tape on risers on existing intruder-resistant security fence.
- Lock operating controls on electrical equipment.
- Commensurate with the assessed risk, insulate MV and LV conductors and connections.

8.3 Kiosk Substations

- Review hazard warning signs and update security signage.
- Lock operating controls on electrical equipment.
- Commensurate with the assessed risk, install dead front electrical equipment.

8.4 Indoor Substations

- Review hazard warning signs and update security signage.
- Lock operating controls on electrical equipment.
- Commensurate with the assessed risk, install dead front electrical equipment.

8.5 Cable Distribution Cabinets

- Review hazard warning signs and update security signage.
- Commensurate with the assessed risk install covers or dead front electrical equipment.