Facilities' physical security upgrade

CP BUS 8.01 - Facilities security - Jan2020 - Public

Regulatory proposal 2021–2026

CitiPower

January 2020

Contents

1 Overview

Business	Powercor and CitiPower
Title	Facilities' physical security upgrade
Project ID	CP BUS 8.01 - Facilities security - Jan2020 - Public
Category	Other non-network capital expenditure IT capital expenditure - recurrent
Identified need	After reviewing our facilities' physical security, we have identified that vulnerabilities exist in the protection of our critical assets that pose risks to the safety of supply, employees and the community.
Recommended option	Option 1: Upgrade security fencing and detection measures
Proposed start date	2021/22
Proposed commission date	2025/26
Supporting documents	1. CP MOD 8.02 - Facilities security - Jan2020 - Public 2. CP ATT048 - BG - Strategic security review - Jun2019 - Public 3. CP ATT049 - Facilities security site implementation - Jan2020 - Public 4. CP MOD 12.02 - Quoted services labour rate - Jan2020 - Public 5. CP ATT200 - ENA - Prevention of unauthorised access - 2006 - Public 6. CP ATT201 - ANZCTC - Protection infrastructure from terrorism - Public

In-line with the company wide review of the security of physical assets, we have identified that vulnerabilities exist in the protection of our critical assets that support the supply of services to the community and safety to individuals.

This business case is driven by a recently undertaken security review (**the Review**), where an independent security consulting company, Bellrock Group, were engaged to assess the current vulnerabilities in our network.[1] As part of the Review, several gaps were identified that must be addressed to strengthen the security and protection to these assets, and to reduce the risk of loss of supply, as well as to protect the safety of employees and the wider community. The Review also aligned with the government's position of critical asset protection.

Three options have been explored within this business case as shown in table 1 below.

Table 1 Options analysis, $m June 2021

	Option	Powercor	CitiPower
0	Do nothing	0	0
1	Address the physical security of highest risk sites	36.2	12.0
2	Address the physical security of all sites	63.1	56.0

Source: CitiPower

Option 1 is the preferred approach, as will reduce customers' energy supply security risk and the potential for harm to our staff and/or members of the public from physical security issues, while ensuring costs remain reasonable for customers.

[1] CP ATT048 - BG - Strategic security review - Jun2019 - Public.

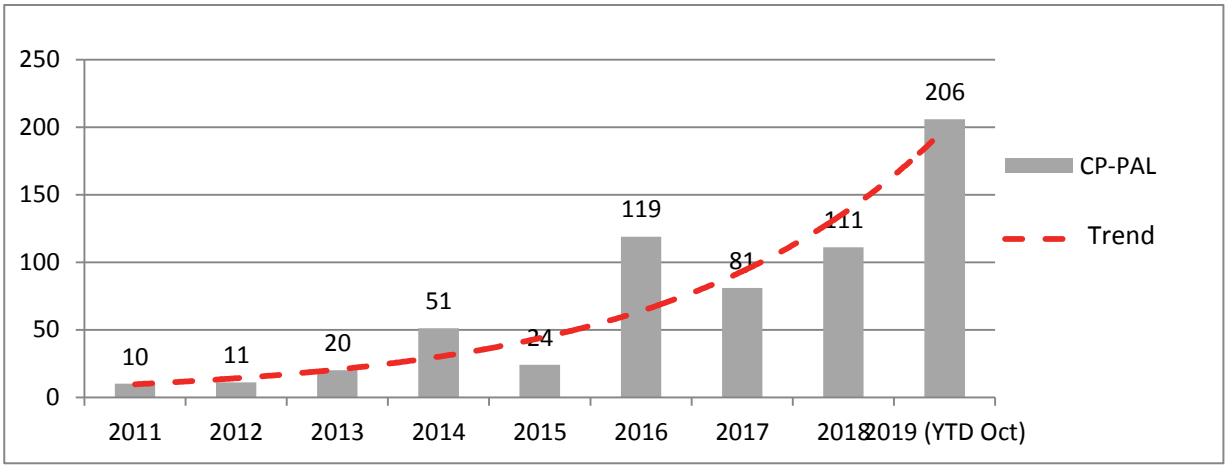
2 Background

2.1 Increasing risks to physical security

The majority of our critical assets (zone substations, distribution assets and depots) are currently protected by rudimentary cyclone fencing, with limited capability to detect or respond to a breach. These sites are being exposed to unauthorised and illegal access, theft and/or damage to equipment and materials.

We are experiencing a general increase in unauthorised access and theft across the network as are other essential services of varying degrees of severity, impacting assets, resulting in thefts and/or impacting the safety and wellbeing of employees.

Figure 1 Number of unauthorised Access Incidents in CitiPower-Powercor



Source: CitiPower

For example, since 2011, there have been more than 400 reported incidences of copper theft across CitiPower and Powercor and more than 30 since January 1, 2019. Our employees have also encountered threats by customers, including in reception areas at depots, and field staff have received abuse during work. We anticipate that without putting new security measures in place that these problems will expand over time, exposing our workers and the communities in which we operate to increasing safety risks.

This has the potential to negatively impact supply of essential services, cause harm to individuals and increase risk of exposure to the public. This requires us to invest to ensure our security measures are suitable to guarantee continuity of supply and mitigate safety risks.

Other distributors have already undertaken security upgrades similar to what we are proposing. For example, United Energy undertook fencing upgrades between 10–15 years ago, and Western Power, received approximately $55m in funding for substation security (including fencing, signage, lighting and active security monitoring) for the 2017/18–2021/22 period.

2.2 Independent security review

Due to escalating concerns that we are at risk of falling below industry standards, our leadership team engaged an independent consultancy, Bellrock Group, to assess the security of our critical assets according to global best practice and to provide recommendations to rectify vulnerabilities in our network.

The scope of the Review involved assessing the physical security of the network including all depots and offices, all zone substations, selected underground and indoor distribution substations in high-risk areas and selected construction project sites in high-risk areas. The Review assessed these assets against the following types of

risks: Environment Risk, Security Risk, Integrity Risk and Political Risk (refer to Appendix 1 - Risk Taxonomy of the Review for further details on risk factors).

Details of Bellrock Group's methodology are summarised further below and detailed in their report.

2.3 Alignment to industry and government guidelines relating to electricity infrastructure

The Review recommendations align where applicable with the Energy Networks Association – National guidelines for prevention of unauthorised access to electricity infrastructure (**ENA Guidelines**), which was developed to support the objectives of the National Electricity Network Safety Code. These ENA Guidelines:

- promote safety as a priority for customers, the public and industry workers
- promote nationally consistent practices
- promote economic efficiencies through standardisation
- simplify the interpretation of regulatory requirements.[2]

The Review aligns with section 6.5.6(a)(iii) of the National Electricity Rules (**the Rules**), which state that a distributor must maintain the quality, reliability, and security of supply of standard control services.

Lastly, the Review also aligns with the government's prioritisation of critical asset protection, which states that:

> *'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'.*[3]

2.4 Physical security program

Following this Review, we have implemented a physical security program with the aim of ensuring the safety of our people, the community, network supply and assets, now and into the future. This program applies industry best practice for physical security solutions and utilises a risk-based and intelligence-led framework. In addition the physical security program focuses on:

- providing a consistent approach for identifying and prioritising critical infrastructure
- providing a consistent assessment and treatment of physical security risks
- identifying specific assets that if immobilised, would result in wide spread community impact
- identifying specific actions and liaison with state emergency response agencies
- providing assurance to asset owners, Governments, customers and community groups of pro-active preventative measures in respect to our critical infrastructure assets.

This physical security program is currently being rolled out and will be applied on an ongoing basis across our assets in the 2021–2026 regulatory period and beyond.

---

2 Energy Networks Association, ENA DOC 015 –2006, National guidelines for prevention of unauthorised access to electricity infrastructure, p 3 (CP ATT200).

3 Australia-New Zealand Counter-Terrorism Committee, National Guidelines for Protecting Critical Infrastructure from Terrorism (CP ATT201).

3 Identified need

Through the Review, we have identified vulnerabilities in the protection of our network that need to be addressed to strengthen the security and protection of these assets and to reduce the risk of loss of supply and public safety in alignment with our physical security program.

The Review noted that we are 'managing some risks well, with good controls in place, and [are] recognised as having a strong commitment from the Executive and Board to improve its security program and underlying culture.'[4] However, it also identified that 'there are some gaps and a lower level of maturity when assessed against the industry and some high security risks across [our network]. This places CitiPower and Powercor at a higher level of risk, potential increased costs, lower operational effectiveness and increased reputation risk, compared to its peers.'[5]

In particular, the current security measures largely provide little defence to unauthorised access with intruders able to readily cut or scale fences in order to gain entry, with limited ability to detect breaches of security or respond. Therefore, it is recommended that additional onsite security measures are required, including the installation of:

- fencing (anti-climb, reinforced fencing)
- monitored security system (to detect intruders and alert us to security breaches)
- hardware upgrades to existing Closed Circuit Television (**CCTV**) and associated servers
- rolling out new CCTV cameras in high risk locations
- a new keying system (current key patent expires 2019)
- improved lighting (motion sensor LED lighting to be used to minimise impact on neighbouring sites)
- a control room to proactively manage all security alerts
- gates control program (upgrading existing technology and adding technology to new, high risk sites).

The upgrades of these assets are discussed further below.

3.1 Zone substation analysis

The Review has identified an extreme safety and supply security concern. This is particularly attributable to people breaking into zone substation assets to seek to cause damage or theft, for example due to ageing fences falling into disrepair. This causes a significant safety risk to those involved, the public and has the potential to impact the continuity of supply to customers.

To assist in managing this risk, we propose to install additional security controls in line with the risk profile determined in the Review and in line with the ENA Guidelines. Security enhancements include installing Gates technology, Fencing, Intruder Detection, new CCTV and lighting.

3.2 Distribution substation analysis

The Review has identified an extreme safety and supply security concern. This is particularly attributable to people breaking into distribution assets to seek to cause damage, theft or reside at sites, for example due to a

[4] Bellrock Group, Strategic Security Review (May 2019), page 4 (CP ATT048).

[5] Ibid.

lack of perimeter detection or response capability. This causes a significant safety risk to those involved, the public and has the potential to impact the continuity of supply to customers.

To assist in managing this risk, additional security controls are required, in line with ENA Guidelines and risk profile, to detect and respond to a breach. This includes enhancing Intruder Detection capabilities.

3.3 Depots analysis

The Review has identified a safety and supply security concern with people breaking into depots to seek to cause damage or theft. This causes a significant safety risk to those involved, employees, the public and has the potential to impact the continuity of supply to customers.

To assist in managing this risk, additional security controls are required in line with the ENA Guidelines. Security enhancements include installing Gates technology, Fencing, Intruder detection, new CCTV and lighting.

3.4 Smart keys project implementation

The Review has identified this area as high risk. We currently rely upon mechanical keys and padlocks as the primary means of preventing unauthorised access to zone and distribution substations and major primary equipment such as ring main units and pole-top switches. The 12-year patents on these keys are due to expire in 2019. From 2019, we will install software, servers and equipment (i.e. key cabinets, keys and barrels) in order to pilot the new system prior to a full program rollout occurring at the start of the regulatory period.

To assist in managing this risk, existing keys and locks should be replaced with a combination of restricted locks and electronic access controlled locks, centrally managed.

3.5 Building Access Control (BAC) maintenance

BAC is an integrated solution that combines the SAP Human Resources systems and the Gallagher security system physical access control system. The Gallagher system provides electronic access and intrusion detection at Depots and Zone Sub Stations.

The integration component allows employee or contractor information to be shared from SAP HR to Gallagher – namely the status of the employee / contractor (active or terminated), and the appropriate competencies for access to distribution properties in line with VESI training and company authorities.

To continue satisfying licence conditions and ensuring the continued effectiveness and integrity of BAC, standard upgrades are required over the forecasting period.

3.6 Gates upgrade

We have identified a safety concern with the current access transmitters used to remotely open gates, as they have a security code that we do not control. This forms a risk of exposure that the codes could be used, disabled or deactivated without our knowledge.

To assist in managing this risk, existing transmitters should be replaced and CCTV system should be extended through integrating with BAC security system, to ensure that personnel have required access, providing greater control and security over entry and exit from sites.

3.7 Control room

We have identified a safety and supply security concern as most of our security is of a passive nature, with the systems controlling access and recording movement. There is no active monitoring of events when unauthorised access occurs.

To assist in managing this risk, a functioning control room should be constructed to utilise existing BAC security system and to actively manage all security alerts arising across the businesses (e.g. 24 hour CCTV monitoring).

3.8 Upgrade existing CCTV infrastructure

CCTV provides a remote view of an installation and can record the activities within its field of view. This is a primary element of recording events and monitoring intruders. Combining CCTV with appropriate security systems and actively monitoring instillations can minimise unauthorised access and reduce the time to respond to incidents and reducing public safety risks.

This initiative will upgrade our existing cameras reaching their end of life so we can ensure continued CCTV coverage of our network.

4 Options analysis

Three options have been explored to determine the solution that best addresses our physical security risks while ensuring cost efficiency.

4.1 Approach

Assess

The Review assessed our needs with the help of internal subject matter experts (**SMEs**) as well as taking into account best practice government and industry standards for electricity infrastructure (detailed in the background section above).

Identify

In the Review, Bellrock Group first identified the likelihood and potential impacts of the following classes of risk:

- Environment Risk.
- Security Risk.
- Integrity Risk.
- Political Risk.[6]

To assess the likelihood of these risks, Bellrock Group considered internal historical data, external historical data from similar industries and the opportunity for the threat to arise, based on internal controls and external circumstances.

Next, in determining how to best address identified risks, the Review sought to prioritise the management of the most important threats (extreme and high), while also establishing a process to monitor the less imperative exposures (moderate, low and negligible). In assessing how to best treat risks, Bellrock group described how the proposed treatment would reduce the threat level of the risk, with reference to global best practice standards.

Compare

We will commence work to address the extreme risk areas identified by the Review in the current regulatory period, with works continuing into the 2021–2026 regulatory period.

We developed and compared three options for the 2021–2026 regulatory period, which progressively build on each other to expand the coverage of our facilities' security capabilities. We took this approach as it allowed us to determine the trade-off between risk and the cost of implementation in order to provide the best value for customers.

In order to accelerate the implementation of Review recommendations, we would need to acquire additional resources above our current workforce, which would add additional costs. To delay implementation would mean prolonging high risk assets. Therefore we did not compare different timings in our options analysis.

Recommend

---

[6] Please refer to Appendix 1: Risk Taxonomy in Bellrock Group, Strategic Security Review (May 2019) for a detailed list of all the risk factors (CP ATT048).

We selected and recommend option 1, providing further detail on the justification in the recommendation section of this document.

Estimate and roadmap

We estimated the recommended option using historical project costs, with adjustments for additional scope where required. We also developed a high-level roadmap over the period 2021–2026 of proposed activities to ensure deliverability of the project.

4.2 Summary

We considered three options for this business case following the approach outlined above. These options are described as follows:

- Option 0 - do nothing to invest in our facilities' security
- Option 1 - address highest risk sites
- Option 2 - address all sites.

Table 2 summarise the total capital expenditure over the five-year regulatory period 2021–2026.

Table 2 Cost analysis ($m June 2021)

	Option	Powercor	CitiPower
0	Do nothing	0	0
1	Address the physical security of highest risk sites	36.2	12.0
2	Address the physical security of all sites	63.1	56.0

Source: CitiPower

4.3 Option 0 – do nothing

Option 1 - do nothing mean we will not install additional security measures. This is not a viable option as it will put our customers' energy supply security at risk and does not reduce the risk of the potential for harm to our staff and/or members of the public by not upgrading security measures.

The advantages and disadvantages of this option are set out in table 3.

Table 3 Advantages and disadvantages of option 0

Category	Advantages	Disadvantages
Safe & Dependable		Reliance on existing physical security capabilities during the 2021–2026 regulatory period will reduce our ability to protect staff and the wider community and detect against unauthorised intrusions, increasing the likelihood of a major security incident at our facilities.
		Increased likelihood that a major physical security incident may result in a failure to deliver a safe and dependable supply of electricity to customers, breaching of section 6.5.6(a)(iii) of the Rules.
Flexible		Unsupported physical security capabilities will not allow us to identify and respond new or emerging security threats. In addition, this approach will not allow us to respond to uplifts in industry best practices for the security of physical assets.
Affordable	No capital expenditure incurred.	Significant costs will be incurred by customers to respond to and remediate physical security breaches, including those resulting from personnel and public injuries.

Source: CitiPower

4.4 Option 1 - address highest risk sites

Option 1 - address highest risk sites – involves implementing the additional onsite physical security measures listed above (see Identified Need) in certain areas. To determine coverage we have used a risk-based approach to identify the highest risk sites, namely those in more densely built up areas. Between 2021/22 and 2025/26 we expect to upgrade 20 zone substations, 50 distribution substations and 13 depots in Powercor and 10 zone substations, 200 distribution substations and 1 depot in CitiPower.

Overall option 1 will reduce customer's energy supply security risk and the potential for physical harm to our staff and/or members of the public in a cost-efficient manner. See CP ATT049 - Facilities security site implementation - Jan2020 - Public for the proposed implementation schedule.

The advantages and disadvantages of this option are set out in table 4.

Table 4 Advantages and disadvantages of option 1

Category	Advantages	Disadvantages
Safe & Dependable	Improves the perimeter security of physical sites Enhances the level of protection to critical assets Provides evidence to be submitted to the authorities in order to identify and prosecute offenders	Facility security not upgraded at all locations
Flexible	Balanced investment option that includes reasonable provisions to address rising security threats according to industry best practice security standards	Higher capital and operational expenditure required compared to Option 1
Affordable	Targets highest risk sites and provides a practical delivery approach Lower capital expenditure per risk reduction than option 2.	

Source: CitiPower

4.5 Option 2 - address all sites

Option 2 - address all relevant sites – involves implementing the additional onsite physical security measures listed above (see Identified Need) in sites across CitiPower and Powercor. Under this approach between 2021/22 and 2025/26 we expect to upgrade 68 zone substations, 205 distribution substations and 13 depots in Powercor and upgrade 85 zone substations, 1955 distribution substations and 1 depot in CitiPower.

Option 2 is the highest cost solution and therefore not the preferred option. However, this approach would have the largest potential to reduce customer's energy supply security risk and the potential for onsite harm to our staff and/or members of the public.

The advantages and disadvantages of this option are set out in table 5.

Table 5 Advantages and disadvantages of option 2

Category	Advantages	Disadvantages
Safe & Dependable	Provides greater reduction in risk of an onsite safety incident occurring to employees or the public from physical security upgrades including from improved site perimeter security and protection to critical assets.	
	Increasing our ability to detect and respond to unauthorised access breaches in a timely manner, before they result in a major safety incident or theft.	
	Provides evidence to be submitted to the authorities in order to identify and prosecute offenders.	
Flexible	Provides alerts for when intrusions occur so that staff operating on site can be alerted and the authorities can be notified	
Affordable		Highest capital and operational expenditure compared to other options.

Source: CitiPower

5 Recommendation

We recommend option 1 as this provides a balanced investment approach for the following reasons:

- **Safe & dependable**: option 1 supports the continued safe, reliable, and secure delivery of electricity.
- **Flexible**: option 1 includes reasonable provisions to address increasing physical security threats according to industry best practice security standards.
- **Affordable**: option 1 reflects a balanced investment in physical security, targeting high risk sites.

Refer to Appendix A for a summary of the associated risks involved in the recommended option and the Review for further detail. We do not recommend the other options for the following reasons:

- option 0 detracts from our ability to ensure a safe and dependable supply of electricity to our customers, and consequently introduce unacceptable levels of risk to the business, our customers, and the community more broadly. Therefore, whilst they may be appealing from an affordability perspective, it is not a viable option.
- option 2 does not provide sufficient additional onsite security benefits given the additional investment, as the existing controls and residual risk are not commensurate to the additional investment required.

Table 6 summarises the expenditure profile for option 1 in the 2021–2026 regulatory period. Note the costs of works forecast to be completed in the current regulatory period are not included. Note that costs are apportioned between our proposed IT expenditure and property expenditure.[7]

Table 6 Option 1: CitiPower and Powercor expenditure profile ($m June 2021)

Expenditure forecast $2020m	2021/22	2022/23	2023/24	2024/25	2025/26	Total
IT capital expenditure	1.7	1.2	1.1	4.1	0.4	8.5
Property capital expenditure	11.6	8.6	7.0	6.2	6.2	39.6
Total	**12.3**	**9.9**	**8.1**	**10.3**	**6.6**	**48.1**

Source: CitiPower

[7] For example, an IT component may relate to back office hardware and server upgrade costs, while the property component relates to the cost of purchasing and installing the capability.

A Risk Taxonomy of the Review

Table 7 Risk taxonomy

Risk Class	Risk Factor	Likelihood of risk	Impact	Primary Rating	Residual Rating[8]
Environmental Risk	Positions and Structure	Expected	Major	Extreme Risk	Moderate Risk
Security Risk	Systems and procedures	Expected	Major	Extreme Risk	Moderate Risk
	Electronic Security	Expected	Medium	High Risk	Moderate Risk
	Security Resourcing	Likely	Major	High Risk	Moderate Risk
	Locking Systems	Expected	Medium	High Risk	Moderate Risk
	Security Culture	Likely	Major	High Risk	Moderate Risk
	Aggressive & Threatening Behaviour	Expected	Medium	High Risk	Moderate Risk
Integrity Risk	Theft	Expected	Medium	High Risk	Moderate Risk

Source: internal analysis of Bellrock Group Strategic Security Review (May 2019) (CP ATT048).

[8] Residual risk following implementation of option 1.