November 2025

Investment Case

Substation Security Uplift Programme

Contents

1 EXECUTIVE SUMMARY

Powerlink is proposing an overall regulated investment of $169.2 million, with $138 million proposed in the 2027 – 2032 regulatory control period to deliver our Substation Security Uplift program. This program will modernise and standardise physical-security controls across Powerlink's substation network, [redacted]

Allocation of Funding - Revenue Period FY28-FY34								
	FY 2028	FY 2029	FY 2030	FY 2031	FY 2032	FY 2033	FY 2034	Total
Regulated Capital Expenditure	$8.0M	$18.0M	$28.0M	$41.0M	$43.0M	$16.3M	$14.9M	$169.2M

Table 1: Summary of Proposed Expenditure

This investment ensures Powerlink meets its legislated obligations under the *Security of Critical Infrastructure Act 2018* (SoCI Act), including enhanced requirements introduced through the *Security Legislation Amendment (Critical Infrastructure) Act*, *Critical Infrastructure Risk Management Program Rules (CIRMP) Rules 2023*, and the *SoCI Enhanced Response Act 2024*. These reforms mandate that critical infrastructure entities identify, assess, and mitigate material physical-security risks, and demonstrate proactive and ongoing security management across their asset base.

Substation sites were separated into three different criticality levels based on objective criteria, focusing on market and network impacts.

- **Criticality Level 1 (C1) -** sites that are necessary for routine operation of Powerlink's transmission network but are not a strategic element of the network and could be worked around if disrupted and result in only low to moderate impacts.
- **Criticality Level 2 (C2)** – sites that are important to Powerlink's transmission network operations and if disrupted would have a moderate to high impact on network integrity and reliability (defined below).
- **Criticality Level 3 (C3)** - sites that are Powerlink's most critical and are essential to transmission network operations and are vital to the integrity of the transmission grid. A disruption to one of these sites would cause significant impacts and a large disturbance on the system with the potential for further cascading effects.

To determine the right mix of mitigations to respond to the SoCI requirements and ensure a proportionate response that balances cost and risk for our customers, Powerlink has undertaken a cost benefit analysis that monetises the benefits of the program to network reliability and asset damage. This CBA demonstrates that differing levels of protection based on the criticality of the site provide the optimum solutions for our customers, with a benefit cost ratio of 2.47 for the preferred option, known as Option 5 throughout this Investment Case. Table 2 outlines the scope of the proposed option.

Table 2: Proposed Solution by Substation Criticality

Item	Low Criticality	Medium Criticality	High Criticality
Replace perimeter fence with a new Electrified chain wire fencing system and concrete plinths where not currently present.			☑
Replace all perimeter vehicle gates with new Welded Mesh gates.			☑
Replace primary pedestrian gate with an electronic access controlled welded mesh gate.	☑	☑	☑
Install electronic access control system to primary vehicle gates.			☑
Install full perimeter CCTV cameras and intruder detection systems from new camera poles.	☑	☑	☑
Harden all operational buildings by replacing all external doors with new steel-clad security doors in addition to installing steel mesh to cover all external windows where present.			☑
Install electronic access control system to all external Operational Building doors where not present or to standard.			☑
Install new internal and external CCTV cameras and Intruder detection systems, [redacted] exterior LED flood lighting to all operational buildings.			☑
Install new Hostile Vehicle Mitigation (HVM) impact rated barriers at the perimeter to protect gates, fences and assets from hostile or negligent vehicle damage.			☑
Rekeying of all site Security locks to new high security restricted master keying system.	☑	☑	☑

2 INVESTMENT NEED

The investment need for the Substation Security Uplift has two key elements:

- **Compliance** – Powerlink has a regulatory obligation to meet the SoCI Act. Internal and external assessments of Powerlink security capability at substation sites have identified that our current systems are below the required level
- **Cost Benefit Analysis** – to determine a proportionate response, Powerlink has developed a cost benefit analysis that quantifies the benefits of differing levels of security capability that still meets minimum compliance. This ensure that Powerlink maximises the benefits to customers from this program of work.

2.1 Background

Powerlink Queensland, as the state's Transmission Network Service Provider (TNSP), is responsible for operating and maintaining Queensland's high-voltage electricity transmission network - a foundational component of Australia's national energy infrastructure. As a Commonwealth-declared critical infrastructure entity, Powerlink has a legislated obligation under the *Security of Critical Infrastructure Act 2018* (SoCI Act) to strengthen and continuously improve physical security controls to manage material risks, prevent unauthorised interference, and ensure the ongoing protection of personnel, assets, and the continuity of essential services.

Major reforms introduced through the *Security Legislation Amendment (Critical Infrastructure) Act 2022* and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act) substantially elevated these obligations. The subsequent *Critical Infrastructure Risk Management Program (CIRMP) Rules 2023* and *SoCI Enhanced Response Act 2024* expanded the definition of critical electricity assets and established prescriptive requirements for how responsible entities must identify, assess, mitigate, and assure material security risks across physical, cyber, personnel, and supply-chain domains.

Historically, Powerlink's security expenditure has enabled the implementation of [redacted], baseline controls. While these measures have delivered a [redacted] level of compliance with the requirements of the time, they have not [redacted] r met the full intent of SoCI obligations. [redacted]

2.2 Problem / Opportunity

[redacted]

Three separate and independent assessments - Project Citadel (2022), O'Connor Marsden & Associates Physical Security Audit (May 2025), and peer benchmarking through the National Transmission Network Security Managers Working Group, supplemented by detailed site-specific vulnerability assessments at Virginia and the Business Continuity Site (BCS)-provide a consistent and compelling view of Powerlink's current physical-security posture. [redacted]

Across all reviews, recurring improvement opportunities were identified [redacted]

[redacted]

[redacted] Investment in physical-security enhancements at substations is therefore necessary to:

- Comply with the SoCI Act and CIRMP Rules through proportionate, risk-aligned controls;
- Support the ongoing delivery of a secure, and reliable electricity transmission service to Queensland consumers, and;
- Reduce the likelihood and consequence of deliberate or criminal interference with critical transmission assets.

2.3 Economically Quantifiable Risks for Powerlink and its Customers

The proposed controls address known vulnerabilities and materially reduce risks across operational, safety, cyber-physical, and community dimensions. This targeted investment enables Powerlink to meet its SoCI obligations, protects the continuity of electricity transmission, and delivers a prudent and proportionate security uplift aligned with the criticality of the assets and the evolving threat environment.

2.3.1 Damage to Critical Equipment

[redacted] cting access to critical components, and enabling early detection of unauthorised activity before damage occurs. This directly lowers the risk of asset degradation, unplanned outages, and capital replacement costs. This benefit has been monetised and been factored into the cost benefit analysis that Powerlink has undertaken to determine the optimum program of work.

2.3.2 Unauthorised Interference with the Network

[redacted] The proposed controls-enhanced perimeter hardening, modern access-control systems, intrusion detection, and centrally monitored CCTV-significantly reduce this risk by preventing unauthorised access, rapidly identifying suspicious activity, and enabling timely escalation and response. This layered approach limits adversary opportunity and materially reduces the risk of intentional disruption or sabotage. This benefit has been monetised utilising the Value of Customer Reliability (VCR) and has been factored into the cost benefit analysis that Powerlink has undertaken to determine the optimum program of work.

2.3.3 Inability to Supply Electricity Services

Security incidents at high-criticality substations have the potential to disrupt electricity transmission, impacting customers, industry, and essential services. By prioritising robust security controls at sites with the highest consequence of compromise and establishing a consistent baseline across the network, the proposal reduces the likelihood that a security event escalates into a supply interruption. Improved situational awareness and response capability further support rapid containment and recovery, strengthening overall network resilience. This benefit has been monetised and been factored into the cost benefit analysis that Powerlink has undertaken to determine the optimum program of work.

2.4 Qualitative Risks for Powerlink and its Customers

2.4.1 Cyber Security Attack Enabled by Physical Access

Physical access to operational technology (OT), communications systems, and control infrastructure presents a credible pathway for cyber intrusion. Strengthening physical security at substations-particularly around control rooms, data centres, and network interfaces-reduces the risk of cyber compromise arising from unauthorised physical access. The proposed controls support a defence-in-depth approach by integrating physical and cyber security, thereby reducing the likelihood of a cyber-physical attack on critical systems. This risk has not been monetised in Powerlink CBA for this program.

2.4.2 Personnel Safety

The enhancement of security controls security control gaps decreases the risk of harm to Powerlink employees, contractors, emergency responders, and visitors. The proposed uplift improves site security, visibility, and response capability, reducing the likelihood of staff encountering unauthorised persons or dangerous situations such as operating unearthed operational/in service equipment, impacted due to theft/vandalism. Clear access controls, improved monitoring, and coordinated incident response also support safer working environments and compliance with Powerlink's duty of care obligations. This risk has not been monetised in Powerlink CBA for this program. Powerlink will continue to assess the potential impact of this and may include these benefits in future CBAs.

2.4.3 Community Safety

Substations are often located near population centres, industrial precincts, and public infrastructure. Security incidents involving unauthorised access, fire, or equipment damage can pose risks to the surrounding community. Enhanced perimeter controls, surveillance, and incident response arrangements reduce the likelihood of such events and improve Powerlink's ability to manage incidents safely and effectively, protecting the community and maintaining public confidence in the secure operation of critical infrastructure. This risk has not been monetised in Powerlink CBA for this program as it would typically be captured in the VCR calculations. However, Powerlink will continue to assess the potential impact of these risks and may include these in future CBA.

3 SECURITY STANDARDS AND APPROACH

Powerlink's proposed protective security investments for the 2027-2032 regulatory period are underpinned by Energy Networks Australia (ENA) DOC 015-2022 – *National Guidelines for the Protective Security of Electricity Networks*. This guideline represents the national, industry-endorsed benchmark for physical protective security across Australia's electricity transmission and distribution sector and has been developed collaboratively by major Network Service Providers, including Powerlink.

3.1 Rationale for Standard Selection

ENA DOC 015-2022 has been adopted as the primary design and assurance standard as it is sector-specific, risk-based, and proportionate, addressing the unique threat profile and operational requirements of electricity transmission assets. Unlike generic security standards, it explicitly considers network reliability, public and workforce safety, protection of SCADA and operational technology environments, and the interdependencies between physical access and cyber risk.

The guideline aligns with ISO 31000 risk management principles and has been updated to reflect contemporary threat conditions and Australia's evolving critical infrastructure regulatory environment, including the *Security of Critical Infrastructure Act 2018* (SoCI Act) and associated amendments.

3.2 Approach to Security Design and Investment

Powerlink applies ENA DOC 015-2022 through a risk-based, Security-in-Depth approach, ensuring security controls are:

- Justified by asset criticality and threat exposure;
- Scalable across diverse asset classes; and
- Proportionate to material risk.

Controls are layered to deter, detect, delay, respond to, and recover from security incidents, reducing reliance on any single measure and strengthening overall network resilience.

The ENA asset zoning framework is used to define baseline security requirements for both energised and non-energised assets, ensuring higher-criticality sites such as substations, control rooms, data centres, and telecommunications facilities receive enhanced protection, while maintaining consistency and efficiency across the broader asset base.

3.3 Regulatory Alignment and Assurance

ENA DOC 015-2022 provides a structured and auditable framework to support Powerlink's compliance with SoCI Rule 11 obligations, including the requirement to mitigate material risks arising from unauthorised access, malicious acts, and physical interference with critical infrastructure.

The guideline integrates protective security within broader corporate governance, enterprise risk management, and assurance processes, providing ongoing confidence that:

- Risks are systematically identified, assessed, and treated;
- Controls remain effective over time; and
- Security investments continue to deliver their intended risk-reduction outcomes.

4 INVESTMENT OPTIONS

4.1 Security Upgrade Options

This investment case considers substantial physical security upgrade program centred on a considered and effective uplift to the physical security posture of substation facilities, to meet compliance obligations under SoCI and CIRMP Rules.

The proposed enhancements are designed to address identified vulnerabilities and threat vectors through a layered, risk-based approach that integrates physical, electronic, architectural, and operational security controls [redacted] critically assessed. Powerlink has identified these as C1, C2 and C3 substation, with C1 least critical and C3 most critical. The enhancements considered are aligned with national guidelines and standards outlined in the ENA Guidelines and the PSPF, with a tailored approach to the asset criticality and threat environment of each Substation.

The range of Powerlink's substation physical security control measure enhancements that have been considered in differing mixtures in the options that we have developed include:

a. **Fencing and Gates**

   i. [redacted]

b. **Electronic Access Control Systems (EAC)**

   [redacted]

c. **Operational Building Hardening**

   [redacted]

d. **CCTV Surveillance Systems**

   [redacted]

e. **Intrusion Detection Systems (IDS)**

   [redacted]

f. **Lighting and Signage**

   [redacted]

g. **Hostile Vehicle Mitigation (HVM)**

i. [redacted]

h. **Rekeying of Facility Locks**

i. Rekeying of all site security locks with a new SCEC rated restricted master keying system and locks

4.2 Regulated and Non-Regulated Cost Split

Powerlink have two distinct asset categories, known as Regulated assets and Non-Regulated assets. Regulated assets are dedicated to supplying Powerlink's regulated customers and form part of the regulated asset base and expenditure to upgrade included in Powerlink's revenue reset. Non-Regulated assets are those dedicated to supplying major customers and generators, with those customers funding the maintenance and upgrade of those assets through their connection charges. It should be noted that many substations have a mixture of Regulated and Non-Regulated assets.

The Substation Security Uplift program spans Powerlink's full asset base. The assets at each substation have been identified as either Regulated or Non-Regulated, with costs attributable the uplift of each substation pro-rated based on this mix. For completeness, Powerlink has included the cost of the full program and outlines the splits between Regulated and Non-Regulated expenditure to ensure only the portion of the uplift attributable to Regulated assets have been included in the analysis.

4.3 Alternatives and Options Analysis

In formulating this investment case, Powerlink identified 5 key options, with Options 3 and 4 having minor alternatives. Figure 2 outlines the options considered and the overall cost for the Powerlink portfolio.

Option 1 All subs to full standard $521,375,965	**Option 2** Only C3 Subs with full standard $134,040,628	**Option 3** All C3 Sites to standard, All operational buildings and access to pedestrian gate to all other sites $233,263,874	**Option 3a** All C3 Sites to standard, All Control buildings and Access Ped gate to half of remaining C2/C1 sites $184,055,628
Option 3b All C3 Sites to standard, All Control buildings and Access Ped gate to C2 Sites only $203,416,253	**Option 4** All C3 Sites and 15 C2 sites to Full standard $184,643,685	**Option 4a** All C3 Sites and 15 C2 Sites To Full Standard plus Perimeter CCTV and Access Ped Gate to All Other sites $261,948,096	**Option 5** (Recommended) All C3 Sites to Full Standard. Perimeter CCTV, detection and Access Ped Gate to All C2 and C1 sites. $226,137,238

Figure 2: Summary of Options Considered

As Figure 2 outlines, the total expenditure for the recommended option is $226 million. The Regulated portion of this program is $169.2 million and is proposed to run over seven financial years. It should be noted that $8.8 million

has also been included in Powerlink's forecast expenditure for 2026 and 2027 for the lead up works for the program. This expenditure has been included in Powerlink's cost pass-through application and the Capex model submitted with its Revenue Reset. Table 3 outlines the yearly split between Regulated and Non-Regulated expenditure for the full program.

Allocation of Funding - Revenue Period FY28-FY34								
	FY 2028	FY 2029	FY 2030	FY 2031	FY 2032	FY 2033	FY 2034	Total
Regulated Capital Expenditure	$8.0M	$18.0M	$28.0M	$41.0M	$43.0M	$16.3M	$14.9M	$169.2M
Non-Regulated Capital Expenditure	$0.0M	$3.5M	$13.9M	$2.5M	$23.3M	$9.9M	$3.8M	$56.9M

Table 3: Summary of Expenditure

As Table 3 outlines, the total Regulated expenditure of the program is $169.2M. The proposed expenditure as part of the 2028 – 2032 regulatory period is $138.0M in Real FY26 dollars. Table 4 outlines the qualitative options analysis that Powerlink has undertaken.

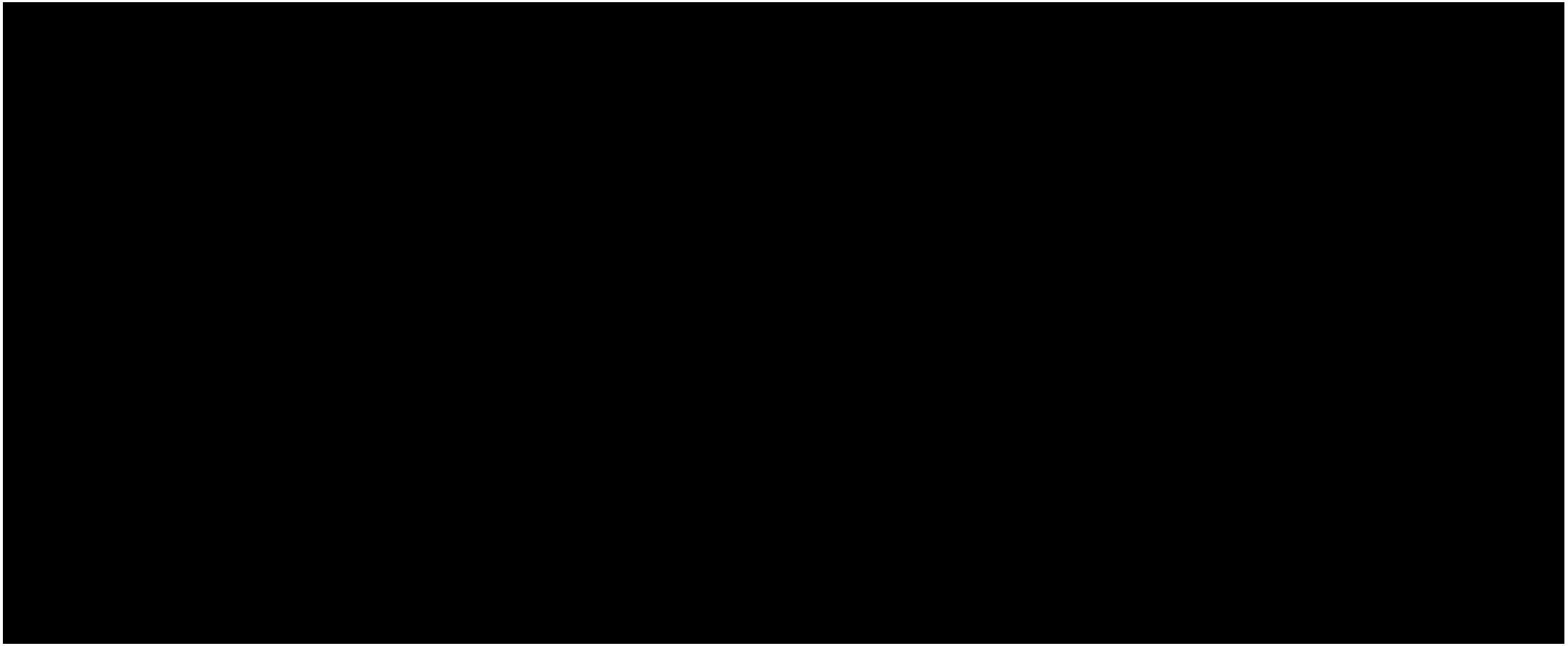


Table 4: Summary of Qualitative Options Analysis

4.4 Cost Benefit Analysis

A cost benefit analysis (CBA) was undertaken to assess the relative benefits of each option outlined in Section 4.3. Powerlink has quantified Network Reliability and Financial benefits as the two key benefits for this program of work. Without intervention, Powerlink's customers would be exposed to a reliability risk from intruders causing network outages, whether deliberately or through theft and vandalism. Additionally, Powerlink and its customers would be exposed to financial costs resulting from the theft and vandalism, or indeed from an action to deliberately damage equipment to cause an outage.

4.4.1 Levels of Intrusion

Three levels of intrusion have been identified

- **Damage / theft** – this is an intrusion for the purpose of stealing property on-site, or for vandalism. This has been assessed as a 10% chance without the program, based on historic data of intrusions. [redacted]
- **Minor Damage** – this is an intrusion for the purpose of causing a network outage through damaging some plant. This has been assessed as a 0.1% probability of occurrence, [redacted]
- **Major Damage** – this is an intrusion for the purpose of causing serious damage and permanent outage of a substation. This has been assessed as a 0.01% probability of occurrence, [redacted]
- **Value of Customer Reliability (VCR)** – the Queensland average VCR of $25,900 / MWh has been utilised to calculate the societal impact of a network outage.

4.4.2 Threat Reduction

This represents the reduction in the number of events that Powerlink expects as a result of the intervention. This has been assessed for the full standard approach, as well as the scale back that is proposed for some options.

- **Theft / vandalism:** it has been estimated that the full Powerlink standard approach will reduce the threat of theft / vandalism at sites by 70%, while the scaled back standard will reduce incidents by 60%.
- **Minor and major damage**: this is assumed to be reduced by 40% for the full measures, and 30% for the scaled back measures

Additionally, Powerlink have also estimated the impact that the security measures will have on changing the outcome of an intrusion:

- **Minor damage** – it has been assumed that for the full measures 20% of incidents will shift from Minor Damage into a theft / vandalism event through the extra active measures Powerlink are able to take. There has been assumed to be a 10% improvement for the scaled back measures.
- **Major damage** – it has been assumed that 20% of incidents will shift to a Minor damage for the full measures and 10% for the scaled back measures.

4.4.3 CBA Outcome

Utilising the key assumptions outlined above, the NPV results are shown in Table 5.

Option	Present Value of Costs	Present Value of Benefits	Benefit Cost Ratio
Option 1 - All subs to full standard	$350,222,417	$426,108,165	1.22
Option 2 - [redacted] with full standard	$95,824,264	$204,433,739	2.13
Option 3 - All C3 Sites to standard. All operational buildings and access to pedestrian gate to all other sites	$160,993,145	$368,581,256	2.29
Option 3a - All C3 sites to standard, All Control buildings and Access Ped gate to [redacted]	$128,673,638	$282,946,377	2.20
Option 3b - All C3 sites to standard, [redacted]	$141,389,512	$341,840,643	2.42
Option 4 - All C3 sites and [redacted]	$129,059,869	$238,389,735	1.85
Option 4a – Addition of security features over Option 4 to remaining 108 [redacted]	$179,832,668	$374,747,091	2.08
Option 5 - All C3 sites to Full Standard. [redacted]	$156,312,438	$385,872,911	2.47

Table 5 – NPV Results

As outlined in Table 5, **Option 5** has the highest cost benefit ratio and provides the highest net benefit to customers.

5 RECOMMENDATION

5.1 Options Analysis Discussion

As outlined in Table 4, all options apart from Option 2 will achieve compliance with SoCI. [redacted] and is not considered an option available for Powerlink to pursue. While all other options achieve compliance with SoCI, the cost for compliance vary significantly.

Powerlink undertook a CBA to quantify the benefits for customers relative to cost for each option. This resulted in Option 5 demonstrating the highest NPV for customers. Powerlink's qualitative assessment also recognised Option 5 as the option that best balanced Powerlink's SoCI obligations, current and future risk exposure and cost to implement.

5.2 Recommended Option

Option 5 is Powerlink's preferred option and aligns with the expenditure that has been included in the revenue submission. This option prioritises the deployment of robust security controls at the network's most critical assets, where the potential consequences of disruption, safety impacts, or service loss are highest. It establishes a [redacted] security standard across all remaining sites, ensuring Powerlink maintains the ability to deter, detect, and respond to security threats in a consistent and measurable manner.

The enhanced use [redacted], integrated with a 24/7 Security Control Room, strengthens situational awareness and enables timely, informed decision-making during security incidents. This capability allows incidents to be assessed and managed in real time, reducing response times and limiting potential escalation or downstream impacts to customers, staff, and the broader community.

Importantly, Option 5 enables a scalable and tiered security model, allowing controls to be uplifted as site risk ratings, threat levels, or business impacts change over time. By applying security controls proportionately across all sites, this approach avoids the creation of security gaps or displacement effects, while ensuring higher-risk facilities receive the level of protection commensurate with their criticality.

Overall, Option 5 provides a balanced, risk-based, and defensible security uplift, aligning regulatory compliance, operational resilience, and community safety outcomes within a sustainable and future-ready framework.

5.3 Preferred Option Detailed Scope

The scope of works that is included in Option 5 from the range of uplifts available are listed below:

a. **Fencing and Gates**

   i. [redacted]

b. **Electronic Access Control Systems (EAC)**

   i. [redacted]

c. **Operational Building Hardening**

   [redacted]

d. **CCTV Surveillance Systems**

   i. [redacted]

e. **Intrusion Detection Systems (IDS)**

   i. [redacted]

f. **Lighting and Signage**

   i. [redacted]

g. **Hostile Vehicle Mitigation (HVM)**

   i. [redacted]

h. **Rekeying of Facility Locks**

   i. Rekeying of all site security locks with a new SCEC rated restricted master keying system and locks (C1-C3)

Appendix 1 – Control Measure Descriptors

In supporting the broader investment case options analysis Powerlink performed a substantially detailed analysis of individual control measure treatments (refer to appendix 2) based on Physical Security standards outline in ENA DOC 015-2022 Guidelines for the Protective Security of Electricity Networks. These options were compared against compliance to the SoCI Act and CIRMP Rules, factoring in various operational, compliance, and resilience impacts for each option.

The analysis enables the comprehensive review of control measure treatments that best satisfy deterrence, delay, and detection requirements while balancing cost, feasibility, and asset criticality. This ensures that investment decisions are defensible, targeted, and proportionate to threat exposure, ultimately strengthening the organisation's protective security posture and regulatory compliance.

1. **Fencing and Gates**

   Considers the standard and configuration of perimeter fencing systems and whether retrofitting of existing fences or full perimeter upgrades are required.

   The preference to rebuild the perimeter fence line to a Category 2–4 Electrified fencing systems was chosen for its ability to deliver a robust layered perimeter protection that significantly enhances deterrence and delay in line with CIRMP obligations.

2. **Electronic Access Control Systems (EAC)**

   Evaluates the level of EAC deployment across facilities and whether access control is applied across all zones or limited to key entry points.

   The option to deploy EAC to all key operational perimeter gates and to all external operational building doors was preferred for its secure, auditable control of personnel movement across critical zones, supporting both compliance to multiple CIRMP Rules and overall operational efficiency.

3. **Operational Building Hardening**

   Focuses on hardening of operational building doors and windows, including full envelope reinforcement or targeted upgrades to primary access points.

   Powerlink chose to replace all external operational building doors with enhanced steel-clad doors proportionate to the security zoning standards in the ENA DOC 2015-22 and installation of SL81 mesh to all exterior windows, offering a cost-effective uplift that meets delay and deter requirements without the need for full structural reinforcement and further supports the deployment of EAC systems.

4. **CCTV Surveillance Systems**

   Considers the extent of camera coverage-whether full perimeter and zone monitoring is implemented or limited to operational buildings and entry points only.

   The option to implement a facility wide Enterprise CCTV cameras system to the perimeter and all operational buildings was selected for its comprehensive monitoring capability that supports real-time threat detection and evidentiary needs across all critical areas.

5. Intrusion Detection Systems (IDS)

Assesses the deployment of Class 4 and 5 IDS across critical zones and buildings, and whether perimeter detection is included or limited to internal areas from operational buildings.

The installation of facility wide IDS was preferred for its early warning capability and layered detection coverage of the full perimeter, enabling timely response and compliance with CIRMP Rules for Detection.

6. Lighting and Signage

Reviews lighting upgrades for visibility and deterrence, and signage for compliance and warning, with options ranging from full site coverage to minimal upgrades at key access points.

The deployment of a facility wide remotely controlled Lighting system and full perimeter security signage was chosen for its enhancement of visibility and deterrence, improving situational awareness and meeting regulatory signage requirements.

7. Hostile Vehicle Mitigation (HVM)

Considers the installation of certified passive and active vehicle barriers at to all perimeter vulnerabilities or limited to access points to prevent ramming or unauthorised vehicular access.

The construction of threat specific Certified passive and active barriers to all perimeter vulnerabilities was chosen for its effectiveness in preventing unauthorised vehicular intrusion and supporting CIRMP compliance for physical access control, Deter and Delay requirements.

8. Rekeying of Facility Locks

Reviews the replacement of existing legacy lock systems with a SCEC-endorsed restricted master keying system to improve access control, auditability, and key management.

Full rekeying of all facility security locks with a new SCEC-endorsed restricted master keying system was preferred for its alignment to the CIRMP Rules and its essentiality to supporting EAC systems providing the most effective solution to access management assurance.

Appendix 2 – Detailed Control Measure Options Analysis

This appendix provides a detailed, structured evaluation and analysis of scalable, risk-led physical security control measure treatments-ranging from fencing and gates to intrusion detection and architectural hardening-aligned with ENA DOC 015-2022 and the obligations under the Critical Infrastructure Risk Management Program (CIRMP) Rules.

PERIMETER FENCING AND GATES

- **Control Consideration 1 – Do Nothing (Status Quo):** Retain the existing fence and commit no investment capital. [redacted] fails to meet the obligations outlined in the Critical Infrastructure Risk Management Program (CIRMP) Rules, and the minimum protective security expectations in ENA DOC 015-2022. [redacted] risks non-compliance with the Security of Critical Infrastructure (SoCI) Act 2018 and its amendments, which mandate proactive risk mitigation for assets deemed critical to national infrastructure. In summary, while cost-neutral, this option exposes the organisation to unacceptable operational, reputational, and regulatory risks and is not recommended for consideration.
- **Control Consideration 2 – Retrofit Existing Fencing:** Retrofitting the existing perimeter fencing with a [redacted] electric fencing system offers a middle-ground solution with lower capital outlay and faster implementation timelines, however the retrofitted solution lacks the structural integrity, uniformity or compatibility required for electric fencing systems and electronic access control which may result in substantial ongoing costs to rectify faults, or result in frequent failure thereby limiting its effectiveness against determined threat actors. Moreover, retrofitting does not address foundational vulnerabilities such as inadequate clearance zones, poor visibility, or lack of reinforced plinths.

  For high-risk substations, where threat vectors include both physical and cyber-enabled attacks, partial upgrades may create a false sense of security and fail to deliver the resilience required under the SoCI framework. While this option may be suitable for low to moderate-risk assets, it is not recommended for critical infrastructure environments without significant supplementary controls.
- **Control Consideration 3 – Replace Existing fence (*Preferred to compliment Option 5 recommendation)*:** This option proposes a full replacement of existing perimeter fencing with a fit for purpose Category 2-4 compliant chain-wire system integrated with [redacted] electrified fencing. It represents a best-practice solution that aligns to CIRMP (Rules 11(1)(d) including relevant standards in ENA DOC 015-2022. Electrified fencing systems not only provide a physical barrier to delay intrusions but also act as a detection and deterrence mechanism, significantly enhancing the site's Security-in-Depth posture. The proposed fencing supports integration with electronic surveillance systems, including CCTV and access control, enabling real-time monitoring and forensic review. The inclusion of concrete anti-dig plinths and clearance zones further strengthens the delay and denial capabilities of the perimeter.

While this option entails higher upfront costs and civil works, these are justified by the substantial uplift in security performance, increased resilience, compliance assurance, and risk mitigation. The investment also supports future scalability and interoperability with enterprise security management systems. For high-risk substations, where the consequences of unauthorised access could include catastrophic safety incidents, operational disruption, and reputational damage, this option provides the most robust and defensible solution. It is strongly recommended for implementation.

ELECTRONIC ACCESS CONTROL (EAC)

- **Control Consideration 1 – Do Nothing (Status Quo):** Retaining the current access control arrangements without enhancement is fundamentally misaligne [redacted] and fails to meet the requirements of the CIRMP Rules, which mandates effective access control for critical assets.

  [redacted]. This option is not recommended.

- **Control Consideration 2 – EAC to Primary Entry Gate and Doors only:** Deploying electronic access control only at primary entry pedestrian gates and operational building doors. While this offers a cost-effective compromise, it introduces inconsistencies in access governance and leaves secondary access points vulnerable. This option may satisfy basic perimeter control requirements but fails to enforce zone-based restrictions within the facility, particularly for areas housing critical operational systems. Without comprehensive coverage, the organisation cannot reliably track personnel movements across zones, nor can it prevent lateral movement by unauthorised individuals once inside the perimeter. This fragmented approach undermines the integrity of the access control framework and may result in partial compliance with CIRMP obligations.

  Additionally, the lack of audit trails for secondary zones impairs incident response and forensic investigation. While this option may be suitable for moderate-risk assets or as a transitional phase, it is not recommended for high-risk substations where full access control coverage is essential to mitigate insider threats, enforce operational discipline, and ensure regulatory compliance.

- **Control Consideration 3 – Full EAC Deployment (*Preferred to compliment Option 5 recommendation)*:** Implementation of electronic access control systems across all critical zones. This option represents a strategic investment in resilience, compliance, and operational integrity. This option enables granular, zone-based access control as outline in ENA DOC 015-2022 standards for electronic access control systems and security zoning methodology, which supports multi-factor authentication (MFA), provides full auditability of personnel movements, real-time monitoring, alarm verification, and remote access management, presenting the most effective method to control and restrict access to critical facilities and components to authorised critical workers, providing multiple alignment to the requirements in CIRMP Rules 9(1)(b), 9(1)(c) and 11(1)(d).

  This option allows the use of secure credential technologies such as MIFARE DESFire EV2 or SEOS, further mitigating risks associated with card cloning and unauthorised duplication. The inclusion of biometric authentication further strengthens identity assurance, particularly for restricted zones housing SCADA

systems and MPLS nodes to allow additional compliance to the AECSF obligations. While the implementation requires infrastructure upgrades, training, and ongoing maintenance, these costs are proportionate to the uplift in security posture and compliance assurance. For high-risk substations, where unauthorised access could result in operational disruption, safety incidents, or national infrastructure compromise, full EAC deployment is the most robust and future-proof solution. It is strongly recommended.

OPERATIONAL BUILDING HARDENING

- **Control Consideration 1 – Do Nothing (Status Quo):** Retain existing perimeter door and window standards for operational buildings [redacted] ENA DOC 015-2022 outlines that building envelopes and internal structures must be designed to resist forced entry, covert intrusion, and environmental degradation. [redacted] From a compliance perspective, this option does not meet the expectations of the SoCI Act or the CIRMP framework. It is not recommended.
- **Control Consideration 2 – Partial Hardening:** Replacing only the access-controlled doors within operational buildings. This option offers a narrowly targeted and cost-effective approach, but it introduces inconsistencies in physical security and leaves other access points vulnerable. This option may include the installation of solid core doors, high-security locksets, and strike shields at primary entry points. While these enhancements improve deterrence and delay at specific locations, they do not address vulnerabilities in walls, ceilings, roof structures, or service openings. As a result, threat actors may exploit alternative entry paths, undermining the effectiveness of the hardened doors.

  Additionally, this approach does not meet the holistic architectural security requirements outlined in ENA DOC 015-2022, nor does it align with the principles of Security-in-Depth. For high-risk substations, where critical systems are distributed across multiple zones, partial hardening may create a false sense of security and fail to deliver the required level of protection. While this option may be suitable for moderate-risk assets or as an interim measure, it is not recommended for critical infrastructure environments without significant supplementary controls.
- **Control Consideration 3 – Full Hardening of windows and doors (*Preferred to compliment Option 5 recommendation*):** This option proposes a focused hardening of the most vulnerable elements of the operational building envelope—specifically doors and windows—without altering the broader structural elements of the facility. The scope includes:
  - **Replacement of all exterior doors** with steel-clad, solid-core security doors compliant with ENA DOC 015-2022 recommendations for secure perimeter access.
  - **Installation of [redacted] steel mesh** or equivalent over all windows to prevent forced entry, aligned with guidance on secured openings and grilles.

This targeted approach directly supports the delay and deter obligations outlined in the CIRMP Rules in addition to supporting effective control and restriction of access. By reinforcing the most common forced entry vectors, the upgraded doors and mesh-covered windows create physical barriers that
Deter unauthorised access by presenting visible, hardened entry points that signal a high-security posture and
Delay intrusion attempts long enough to enable detection and response, thereby reducing the likelihood of successful asset compromise. The solution is scalable and suitable for assets rated as moderate to high criticality, particularly where full structural hardening is not feasible or justified. It delivers measurable uplift in protective security posture and aligns with the principles of Security-in-Depth and risk-based treatment planning outlined in the ENA Guidelines.

CCTV SURVEILLANCE SYSTEMS

- **Control Consideration 1 – Do Nothing (Status Quo):** [redacted] ENA DOC 015-2022, which emphasises the role of video surveillance in strengthening Security-in-Depth, supporting incident investigation, and enabling remote monitoring.

  [redacted] In the context of the Security of Critical Infrastructure (SoCI) Act and CIRMP obligations, this option is non-compliant and exposes the organisation to reputational, operational, and compliance risks. It is not recommended.

- **Control Consideration 2 – CCTV to Operational Buildings only:** This option proposes the installation of CCTV cameras exclusively to monitor the external access points, immediate surroundings and interior of operational buildings. While this approach offers a limited improvement in situational awareness, it does not provide adequate surveillance of the perimeter fence line or access gates needed to support perimeter intrusion detection systems at the earliest point of possible intrusion, which is essential for effective detection and response. In addition, it lacks the ability to provide visual verification of persons entering the facility via access gates for auditing and investigation purposes. As such, this option does not adequately support the principles of Security-in-Depth, nor does it meet the delay and deter obligations under the CIRMP Rules, which require layered detection and deterrence capabilities across all critical zones.

  This option may be suitable for moderate-risk assets or as a transitional phase where budget or infrastructure constraints prevent full perimeter coverage. However, for high-risk substations, where perimeter breaches can result in operational disruption or safety incidents, this option is not recommended as a standalone solution.

- **Control Consideration 3 – Full facility CCTV Upgrade (*Preferred to compliment Option 5 recommendation*):** This option proposes a comprehensive upgrade to a full-scale Enterprise CCTV network deployment to meet the standards outlined in AS/NZS 62676 and ENA DOC 015-2022**.** It includes the implementation of high-resolution cameras configured to achieve targeted standards for identification, recognition, and observation across all critical zones. Cameras will be strategically positioned to cover entry/egress points, perimeters and critical sub-components with illumination designed to optimise image quality under all lighting conditions.

The cameras will be integrated to the enterprise [redacted] Security System, enabling real-time monitoring, alarm verification, and remote response. Recording subsystems will be fully redundant and sized to retain recorded hi-resolution footage of all cameras, ensuring compliance with evidentiary and audit requirements. This upgrade supports intelligent video analytics, enabling proactive threat detection and enhancing situational awareness. While the capital investment is substantial, it is justified by the uplift in operational capability, compliance assurance, and risk mitigation. For high-risk substations, where visibility and response time are critical, this option provides the most robust and defensible surveillance solution. It is strongly recommended.

INTRUSION DETECTION SYSTEMS (IDS)

Control Consideration 1 – Do Nothing (Status Quo): Maintain existing state of [redacted] to meet the expectations outlined in ENA DOC 015-2022, [redacted] In the context of the SoCI Act and CIRMP obligations, [redacted], this option [redacted] is not recommended.

Control Consideration 2 – IDS Coverage for Operational Buildings Only (*Preferred to compliment Option 5 recommendation)*: This option proposes the installation of intrusion detection systems exclusively to and within operational buildings. While this approach enhances detection capability within critical internal zones, it does not provide coverage of the perimeter fence line or external compound areas, which are the first points of compromise in substation intrusion scenarios. As such, this option does not fully satisfy the delay and deter obligations under the Critical Infrastructure Risk Management Program (CIRMP) Rules, which require layered detection and deterrence across all critical zones to prevent unauthorised access and enable timely response. This option may be suitable for moderate-risk assets or as a transitional phase where budget or infrastructure constraints prevent full perimeter coverage. However, for high-risk substations, where perimeter breaches can result in operational disruption or safety incidents, this option is not recommended as a standalone solution.

Control Consideration 3 – Full IDS Deployment (Preferred): This option proposes the deployment of fully integrated Class 4 and Class 5 intrusion detection systems across all zones starting from the perimeter of the facility in the form of Radar motion detection sensors, thermal monitoring cameras with advanced analytics, Electronic fence detection systems and Passive infrared sensors, in accordance with AS 2201 series standards and ENA DOC 015-2022. Class 4 systems provide robust perimeter and facility protection, while Class 5 systems are designed to detect insider threats and sophisticated intrusion attempts. The IDS will be seamlessly integrated with the enterprise security management systems, enabling real-time alarm generation, assessment, and response coordination. The system will also maintain an auditable alarm history for evidentiary and compliance purposes. This deployment supports proactive threat detection, reduces response times, and enhances situational awareness. While the capital investment is significant, it is proportionate to the uplift in security posture, regulatory compliance, and operational assurance. For high-risk substations, full IDS deployment is essential to mitigate both external and internal threats and is strongly recommended.

HOSTILE VEHICLE MITIGATION (HVM)

- **Control Consideration 1 – Do Nothing (Status Quo):** Maintain existing state of [redacted] may result in non-compliance with the SoCI Act and associated risk management obligations. This option is not recommended.
- **Control Consideration 2 – Limited Hostile Vehicle Mitigation:** Installing hostile vehicle barriers only at primary entry points. This option offers partial protection but leaves other vulnerable perimeter sections exposed. While this may deter casual or opportunistic threats, it does not address high-speed ramming or off-road access attempts. ENA DOC 015-2022 recommends comprehensive perimeter protection for assets rated as high criticality. This option may be suitable for moderate-risk assets or as a transitional phase, but it is not recommended for critical infrastructure environments where full perimeter integrity is essential.
- **Control Consideration 3 – Full Hostile Vehicle Mitigation Deployment *(Preferred to compliment Option 5 recommendation)*:** This option proposes the deployment of certified hostile vehicle mitigation systems to the perimeter of substation facilities tailored to site-specific vulnerabilities and operational requirements. Measures include:
    - Passive barriers: Static bollards, Armco (w-beam), and jersey barriers.
    - Active barriers: Hydraulically operated bollards, rising steps, and motorised arm barriers.

  All systems will be [redacted] standards and active barriers integrated with access control systems. Safety loops, redundant power supplies, and traffic lights will be included to ensure operational safety and compliance. This approach provides robust protection against vehicle-borne threats, supports perimeter integrity, and enhances deterrence. It also aligns with ENA DOC 015-2022 recommendations for high-risk assets and supports compliance with critical infrastructure legislation. For substations and control buildings with public road exposure or limited stand-off, full deployment is strongly recommended.

LIGHTING AND SIGNAGE

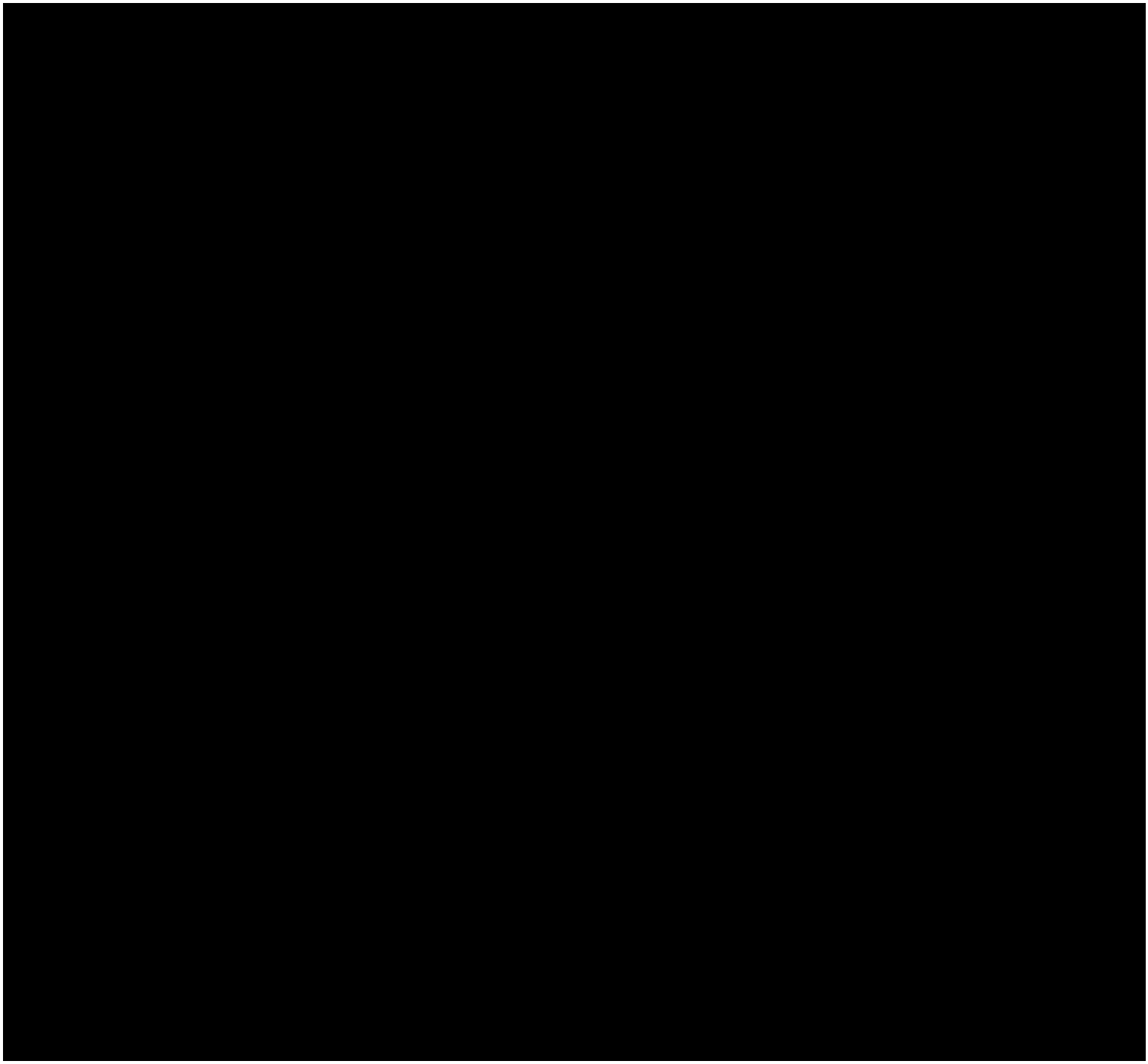
- **Control Consideration 1 – Do Nothing (Status Quo):** [redacted]. ENA DOC 015-2022 outlines that lighting should be designed to eliminate shadows, support surveillance systems, and ensure safe access and egress. Signage must be clearly visible, mounted at eye level, and include hazard warnings and contact information. Without these enhancements, the site remains non-compliant with duty-of-care obligations and vulnerable to both external and internal threats. This option is not recommended.
- **Control Consideration 2 – Lighting and Signage at Entry Points Only:** Enhancing lighting and signage only at primary entry points. This offers a minimal uplift in deterrence and compliance but fails to address vulnerabilities across the broader facility. While this may improve visibility and hazard communication at key access points, it leaves perimeters, operational zones, and emergency exits inadequately illuminated and unsigned. This fragmented approach does not meet the holistic requirements outlined in ENA DOC 015-2022,

which emphasises full coverage to support surveillance, access control, and emergency response. Incomplete lighting can impair CCTV performance and create blind spots, while insufficient signage may result in legal exposure and public safety risks. This option may be suitable for moderate-risk assets or as a transitional phase, but it is not recommended for critical infrastructure environments.

- **Control Consideration 3 – Full Lighting and Signage Upgrade (*Preferred to compliment Option 5 recommendation*):** This option proposes a comprehensive upgrade of facility lighting and perimeter security signage, aligned with ENA DOC 015-2022 and AS/NZS 4282:2019 standards. Lighting will be designed to support CCTV and intruder detection systems, allowing remote activation to eliminate dark zones, enhancing natural surveillance and target identification for detection and response. In addition to security it provides a key safety focus in supporting field operational teams and emergency services in navigating site hazards. Signage will be installed at all entry points, and perimeters, clearly communicating legislative powers for unauthorised site access, site access process, and site identification. This upgrade improves deterrence, supports incident response, and ensures compliance with safety and regulatory standards. It also enhances the perception of site control and professionalism, contributing to a stronger security culture. For high-risk substations, where visibility and hazard communication are critical, this option is strongly recommended.

REKEYING OF SUBSTATION SECURITY LOCKS

- **Control Consideration 1 – Do Nothing (Status Quo):** Retain the existing aging legacy keying system. [redacted] risks non-compliance with the CIRMP Rules, particularly in relation to access control, deterrence, and delay. This option is not recommended
- **Control Consideration 2 – Partial Rekeying:** This option involves either, a) rekeying only C3 categorised substations or, b) targeted rekeying of only Operational Buildings across all Powerlink Substations using a restricted master keying system. While it introduces some access control improvements to either the Highest critical sites or of Critical Components within operational buildings, either option lacks consistency essential to HV operational environments or effectively addressing the risk of bypassing access controls to unkeyed vulnerable high-risk assets, which me result in noncompliance to the standards required under the CIRMP Rules. This option may be suitable for low-criticality assets or as a temporary measure, but it is not recommended for HV operational environments or of any operational buildings containing Critical subcomponents.
- **Control Consideration 3 – Full Rekeying of all substations *(Preferred to compliment Option 5 recommendation):*** This option proposes a complete rekeying of all perimeter and operational building security locks using a SCEC-endorsed restricted security master keying system. This will allow a regained and fully centralised control and management of access to all Substation facilities using a scalable, high security keying system with Restricted key profiles to prevent unauthorised duplication, Hierarchical access control via GGMK structure, Audit-ready key issue and return records maintained in a centralised database, providing a high level of key management assurance.



The CAPEX estimates presented in this investment case have been developed using a bottom-up costing approach, informed by:

- Historical pricing data
- Market engagement with multiple suppliers
- Internal quantity surveying and benchmarking against similar infrastructure projects

All estimates are subject to final validation through competitive tendering and contract negotiation. Escalation assumptions are based on CPI forecasts and sector-specific inflation trends.

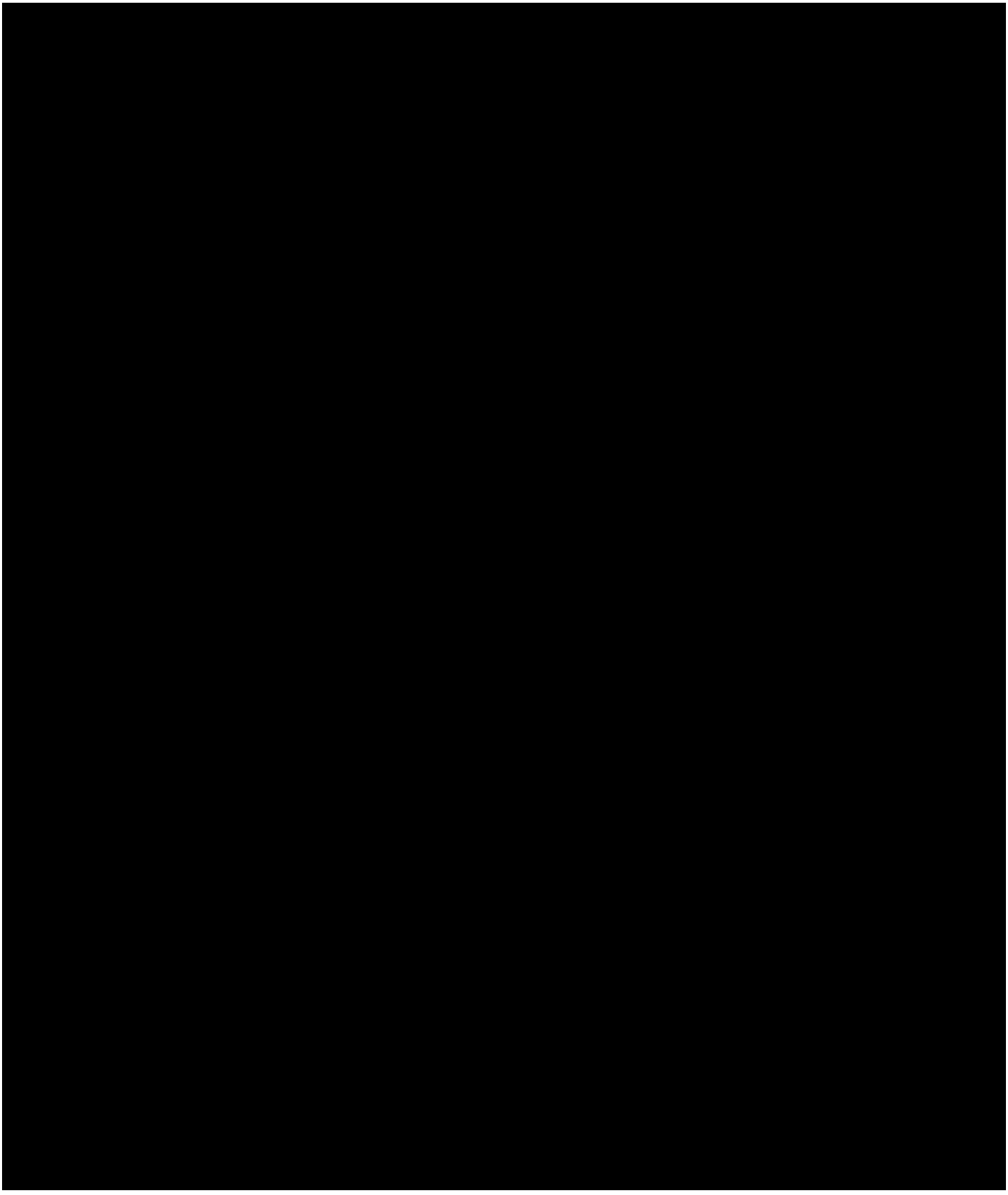
Appendix 4 – Glossary of Terms

Term/Acronym	Description
SoCI Act	Security of Critical Infrastructure Act 2018 (Cth) – Primary law requiring security risk management for critical infrastructure sectors (amended in 2021 and 2022 to increase obligations). "Cth" denotes Commonwealth of Australia (federal law).
SLACIP Act	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth) – Key amendment to the SoCI Act that introduced mandatory Risk Management Programs for critical infrastructure. Came into effect April 2022. Often referred to as the "SoCI Act amendments 2022."
CIRMP	Critical Infrastructure Risk Management Program – A systematic plan and set of controls that a responsible entity (like Powerlink) must have, covering how it will manage security risks (cyber, physical, personnel, supply chain). Required under the SoCI Act amendments. Also refers to the written document outlining that program.
CIRMP Rules	The detailed Critical Infrastructure Risk Management Program Rules issued by the Dept. of Home Affairs (Feb 2023) that specify requirements for CIRMP (e.g., what must be included, specific outcomes like "deter, detect, etc."). These Rules have legal force and guide compliance.
TNSP	Transmission Network Service Provider – An entity that owns/operates high-voltage transmission lines and network (e.g., Powerlink). TNSPs are regulated by the AER for their monopoly services.
Project Citadel	Internal name for Powerlink's 2022 security gap assessment project. Essentially the internal review that identified security improvements needed (used to inform this investment case). "Citadel" signifies fortress, reflecting the aim to bolster defences.
VPN	Virtual Private Network – Secure communication tunnel over the internet or shared network. We may use VPN connections for secure data transmission from remote sites to control centre if needed.
UPS	Uninterruptible Power Supply – Battery backup system to keep equipment running during short power outages or until generators kick in. The security control centre and some field devices will use UPS units for resilience.
PTZ Camera	Pan-Tilt-Zoom camera – A type of CCTV camera that can be remotely controlled to pan (move horizontally), tilt (move vertically), and zoom in on areas of interest. Useful for actively monitoring large areas.
HVM Barriers	Hostile Vehicle Mitigation barriers – Physical barriers (like bollards, reinforced gates) designed to prevent or slow down vehicle-based attacks (e.g., ramming a truck into a facility). Being added at key entrance points where applicable.
HV	High Voltage – Not spelled out in text, but context of substations etc., HV stands for the high voltage network components
DSP	Design Service Providers – Contracted to perform detailed design, preliminary construction assessments, quantitative surveying, construction SOW documents.

Appendix 5 – References/ Data Sources

The following reference material is relevant to this document:

References
Australian Security Intelligence Organisation (ASIO) National Threat Assessment (2025-2030)
Critical Infrastructure Risk Management Program (CIRMP) Rules (February 2023)
Energy Networks Australia (ENA) DOC 05-2022 – National Guidelines for Protective Security of Electricity Networks
Powerlink "Project Citadel" Security Assessment Report (2022)
Powerlink Security of Critical Infrastructure (SOCI) Risk Management Program (RMP) – Framework
Powerlink Protective Security Strategy (ASM-STR-A5860964)
Security of Critical Infrastructure Act 2018 (Cth)
Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth)
Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)
Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (Cth)
Queensland Government Energy Security Statements/Press (2022)



Contact us

Registered office	33 Harold St Virginia Queensland 4014
	ABN 82 078 849 233
Postal address	PO Box 1193 Virginia Queensland 4014
Telephone	+61 7 3860 2111 (during business hours)
Email	pqenquiries@powerlink.com.au
Website	powerlink.com.au
Social	