Jemena Electricity Networks (Vic) Ltd

IT Investment Brief – Cyber Security Program

Non-recurrent – Maintain and Compliance

Glossary

ACSC	Australian Cyber Security Centre
AESCSF	Australian Energy Sector Cyber Security Framework
Capex	Capital Expenditure
CASB	Cloud Access Security Broker
Current regulatory period	The period covering 1 July 2021 to 30 June 2026
CYxx	Calendar Year xx – the period covering January to December
IAM	Identity Access Management
ICT	Information and Communications Technology
IoT	Internet of Things
ISO	International Organisation for Standardisation
Jemena	Refers to the parent company of Jemena Electricity Network
JEN	Jemena Electricity Network (Vic) Ltd.
Next regulatory period	The period covering 1 July 2026 to 30 June 2031
NIST	National Institute of Science and Technology
NPV	Net Present Value
Opex	Operating Expenditure
PAM	Privileged Account Management
RYxx	Regulatory year covering the 12 months to 30 June of year 20xx for years in the Next Regulatory Period. For example, RY25 covers 1 July 2024 to 30 June 2025
SDLC	Systems Development Life Cycle
SOCI	Security of Critical Infrastructure Act
Totex	Total Expenditure

Cyber Security Program

Objective	The objective of this initiative is to deploy capabilities in step with technology advancement that provide fit-for-purpose protection and response in line with cyber security threats, supporting Jemena Electricity Networks Vic Ltd. (JEN) in promoting efficient, safe and reliable service delivery to customers.		
Non-recurrent ICT sub-categorisation	☒ Maintaining existing services, functionalities, capability, and/or market benefits	☒ Complying with new/altered regulatory obligations/requirements	☐ New or expanded ICT capability, functions, and services

Background

Cyber security is an increasingly prominent threat

Cyber security risks continue to challenge companies in Australia and across the critical infrastructure sector. In 2022, cyber incidents reported to the Australian Cyber Security Centre (ACSC)[1] have seen the utility sector move into the top 10 industries based on the volume of reported incidents. The 2022-23 Cyber Threat Report published by the Australian Signals Directorate (ASD) in November 2023[2] highlights that the number of cyber incidents in Australia are maintaining their upward trend. In FY23, approximately 94,000 cyber incidents were reported to the ASD, a 24% increase from the 76,000 reported the previous year and a rate of growth that greatly outstrips the growth in operating businesses. In the same period, 143 cyber security incidents were related to critical infrastructure operational technology and across Australia, significant data breaches resulted in millions of Australians having their information stolen.

Cyber threats are expected to continue to increase, with Gartner[3] predicting that by 2025, 30% of critical infrastructure worldwide will experience a breach that will result in the halting of either operations or mission-critical cyber-physical systems. [redacted]

Ensuring robust cyber security is crucial for maintaining business continuity

Jemena implements a comprehensive, enterprise-wide cyber security program, allowing JEN's customers to benefit from a more cost-effective system by distributing costs across a wider range of businesses and ensuring maximum cost efficiency.

Jemena adopts a risk-based approach to cyber threats

Jemena uses the National Institute of Science and Technology (NIST) Cyber Security Framework and the Australian Energy Sector Cyber Security Framework (AESCSF) to assess its cyber-security risk and has an appropriate level of maturity when measured against these frameworks.

In addition to these frameworks, we use threat intelligence from Government and commercial organisations to inform the planning and implementation of appropriate controls and risk-reduction strategies. This approach allows us to deploy controls based on current techniques, tools and procedures used by adversaries today and into the future. Jemena currently uses general cyber security threat intelligence services from ASD/ACSC and CrowdStrike, with Operational Technology (OT) specific intelligence provided by Dragos. As products and vendor offerings around security evolve, we may change systems over time.

Jemena's risk-based approach to assessing and managing cyber threats

[redacted]

Jemena applies integrated risk management practices [redacted] there

[1] ACSC July 2021 – June 2022 Annual Cyber Threat Report | ACSC (cyber.gov.au)

[2] ASD Cyber threat report 2022- 2023 | ASD (cyber.gov.au)

[3] Gartner predicts 30% of critical infrastructure organisations will experience a security breach by 2025 | Gartner (gartner.com)

are several related frameworks, manuals and procedures we adopt to manage risk and cyber threats, including:

[redacted]

Cyber risk assessments consider government and industry security threat intelligence and information regarding the unprecedented volume of reported cyber incidents and the gravity of impacts on companies, the community, and individuals.

Recognising the inextricable link between energy security and the management of the electricity system and markets, the Minister[4] is now proposing the Australian Energy Market Operator deliver additional cyber security functions related to cyber incident response, preparedness, risk and advice.

Jemena considers cyber threats a key contributor to its top operational risks impacting the safe and secure supply of JEN services (refer to Attachment A). As a result, Jemena continually assesses and updates cyber security capability to respond to threat information.

Jemena's cyber security controls

Jemena has a mature and stable cyber security function with ongoing recurrent investment that allows us to manage known risks. Refer to Attachment B - Jemena's Cyber Assurance Framework.

By continually assessing threat intelligence, Jemena has increased its cyber security capability over the past five years, investing in staff and technology to implement key controls as outlined in the table below.

Table 1: Cybersecurity capabilities

Key Control	Objective / Description
User Awareness	User awareness aims to improve security through mitigating human error, protecting against social engineering and phishing attacks, enabling early threat detection and reporting, ensuring compliance with regulations, and safeguarding the company against malicious attack.
Mail Filtering	Blocks targeted inbound email attacks including credential phishing, business email compromise and supply chain fraud.
Managed Detection and Response	Managed detection and response (MDR) is a cyber security service that combines technology and human expertise to perform threat hunting, monitoring, and response of end-point devices. MDR enables rapid identification and response to limit the impact of threats.
Network Segmentation	Network segmentation involves partitioning a network into smaller networks with an aim to restrict the level of access to sensitive information, hosts and services.
Vulnerability Management	Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

[4] Rule Change request, Australian Energy Market Operator – Cyber Security Role, March 2024 | Australian Government DCCEEW (AEMC.gov.au)

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>Zero Trust Exchange</td><td>Isolates network connectivity limiting exposure of services directly to the internet, reducing risks of Distributed denial of service attacks</td></tr>
<tr><td>Geographical Blocking</td><td>Automatically restricts access to the corporate system making them accessible from with the Australian geographic region only</td></tr>
<tr><td>Identity Management</td><td>Limiting, authorising and managing access to enterprise resources to keep systems and data secure</td></tr>
<tr><td>Security Incident Response</td><td>Planned response in preparation to monitor, contain, eradicated bad actors or malware resulting from a cyberattack</td></tr>
<tr><td>System Backup</td><td>Backups enable recovery of systems and encrypted or lost data</td></tr>
<tr><td>Disaster Recovery</td><td>Plans, processes and capability to restore Digital systems and data after an event that disrupts Digital operations, such as a natural disaster, a cyberattack, or a hardware failure.</td></tr>
</table>
<p>Looking ahead to the 2026-31 regulatory period, cybersecurity will be a key investment priority for JEN. A successful breach or incident could seriously compromise the safety and security of our distribution system and the services we provide to customers.</p>
</td>
</tr>
<tr>
<td>Customer Importance</td>
<td>
<p>An extensive customer engagement program was implemented with JEN residential customers, small and medium businesses, large commercial and industrial customers, stakeholders, and energy experts to shape the 2026-31 Draft Plan. Key customer priorities on how we should prepare for a more sustainable energy future while meeting customer and community needs today from customers includes:</p>
<ul>
<li><b>Affordability</b> - Affordability is a key priority for customers who face impacts from the rising cost of living and inflation. Customers want us to consider affordability over the short and long-term when making decisions.</li>
<li><b>Resilience and reliability</b> - Customers want a reliable and resilient network that can withstand and recover from the impacts of more extreme weather events.</li>
<li><b>A sustainable future</b> - Customers want us to help drive sustainability within JEN and support renewable energy solutions where possible. Customers want us to have sustainable operations and lead the way in meeting emissions reduction targets.</li>
<li><b>Digitisation and automation</b> - Customers want JEN to digitise and automate the grid to make it a smarter and more efficient network.</li>
<li><b>Accessible communication</b> - Customers value efficient and accessible communication and want to easily access information on our service and the customer service team easily.</li>
<li><b>Fairness</b> - Customers want us to consider fairness in the context of the energy transition and its impacts on both existing and future generations, and on our more price-sensitive customers</li>
<li><b>Education</b> – Customers want us to improve and enhance our education to customers on what we do, energy saving tips, the energy transition and Consumer Energy Resources (CER).</li>
</ul>
<p>ICT is a primary enabler of JEN's ability to operate a safe, reliable, and efficient distribution network. Cyber security risk is the most probable harm that could cause the widest possible impact on the safe and reliable delivery of electricity to our customers.</p>
<p>The energy industry, including electricity distribution networks, is particularly exposed in the event of a cyberattack due to the criticality of the services provided. Given the nature of Jemena's business, a cyber-attack on Jemena’s ICT systems, whether targeted, opportunistic, or indirect, will have a significant customer impact if not managed effectively:</p>
<ul>
<li>Smart network devices, if taken control of remotely by malicious attackers, could impact the supply of electricity, cause damage to equipment and expose the public to safety risks. Smart meters can be hacked to alter usage data, allowing customers or intruders to manipulate bills and usage statistics. Cybercriminals may even use compromised accounts to steal electricity or resell it illegally.</li>
<li>Customers increasingly have IoT-connected appliances and renewable energy devices integrated into the grid. If attackers hijack these devices, they could access the broader grid or manipulate individual energy usage, impacting billing accuracy or even damaging connected devices.</li>
</ul>
</td>
</tr>
</table>

- As smart meters and home energy management systems become common, customer data such as usage patterns, billing information, and personal identifiers become valuable. Attackers may breach company systems to steal this data, leading to identity theft and privacy invasions. The theft of sensitive customer data could also adversely affect customers and reduce trust in JEN.
- Spoofing of work orders and instructions to field staff could result in JEN workers unknowingly causing impact services on parts of the network that only support the manual operation.
- If computer systems relied upon by field and office staff are disabled, JEN will lose the ability to operate its business, which may impact the integrity of customer billing, resulting in longer outages and increased operating costs.

JEN's priority is to maintain the supply of electricity, operate a safe and reliable energy network and protect customer data and information.

To meet customer expectations for safe and reliable electricity supply Jemena must continue to invest in capability to identify, protect, detect, respond and recover from cyberattacks.

Key Considerations

Continued investment in Cyber Security is required to keep pace with cyber threats

Advancements in the technology areas of data analytics, cloud adoption and smart integrated networks are quickly transforming how assets and ICT processes are applied and operated.

Digitisation and cloud adoption are forcing companies to shift away from traditional ICT perpetual licensing and owner-operator models from the past to technology services hosted externally and maintained by external 3rd parties, driven through operating efficiencies and reduced total cost of ownership benefits. The autonomous nature of smart devices, their interdependency with ICT systems and their growing reliance on 3rd parties through digitisation are creating blind spots and increasing the potential for ICT exposure and exploitation by cyberattacks.

Technology advances benefit company efficiency and generates opportunities for cybercriminals to apply new tactics, tools, and processes. Jemena must continue to deploy cyber security capabilities with technological advancements that provide fit-for-purpose protection and response in line with current and emerging cyber security threats.

As trends in cyber security threats grow, so do government laws, rules and regulations aimed at protecting consumers subjected to those risks. This parallel trend means that Jemena needs to meet the actual threat as well as the expectations placed on it by governments in the next regulatory period.

[redacted]

To meet customer expectations for safe and reliable electricity supply [redacted] Jemena must continue to invest in systems to identify, protect, detect, respond and recover from cyberattacks.

With our ongoing program to maintain existing cyber security capabilities, this investment brief proposes a threat-based and risk-based approach to uplifting JEN's cyber security capabilities to minimise and mitigate increasing cyber security threats.

How costs were derived

In deriving costs we have assumed internal labour, leveraging the expertise of our cybersecurity team, who understand the new functionalities required.

Since all components of the project are cloud-based, the associated project costs are classified as opex.

The cost estimation process leveraged insights gained from extensive discussions with vendors, including [redacted] who provided input on indicative pricing specifically for licensing.

Recurrent step opex comprises costs associated with new licences for CASB, Privileged Access Management and Privileged Identity Management. An existing license is in place for Identity Access Management and pricing accounts for incremental increases of the existing license.

Options

JEN has considered two options to deliver the capability articulated above:

(1) Maintain existing cyber security controls

(2) Implement incremental fit-for-purpose cyber security controls to continue managing existing and emerging cyber threats.

Whilst considering the options, we explored a third option of delaying any projects by a year, to minimise the upfront investment needed in the 2026-31 regulatory period. The impact on JEN and our customers is too high to consider this option as viable. Delaying by a year could expose JEN to significant cyber risks, leaving our systems outdated and vulnerable to security breaches. This deferment could lead to increased susceptibility to cyberattacks, data loss, and non-compliance with emerging regulations, ultimately compromising our operational integrity and market trust.

Option 1: Maintain existing cyber security controls

Description

Maintain our existing cyber security controls (refer to the Background section) which are covered under operating expenditure. No additional capability will be implemented to mitigate against increasing cyber threats as assessed as part of our CI Risk Management Plan.

Benefits

Expenditure levels are maintained, with no short-term additional operational expenditure outlay.

Risks

Taking this approach materially increases the likelihood of a successful cyberattack that impacts the safe supply of electricity to our customers. Over time the probability of success increases as the gap widens between control effectiveness and threats as controls become out of step with criminal tactics. Doing nothing has the safe effect of reducing control effectiveness over time.

Jemena considers the risk rating of maintaining the status quo to be high due to increased vulnerabilities.

[redacted]

Summary

This option is not recommended. It will expose JEN to an increasing likelihood of a successful cyberattack with network and customer implications, and JEN considers that it does not reflect good industry practice.

Option 2: Implement fit-for-purpose cyber security controls

Description

In addition to maintaining our existing cyber security controls, the cyber security program comprises several additional security capabilities, all of which will contribute to the continued security of the JEN network, systems and data. These are described further below:

- Zero trust is a security model that ensures secure cloud passage through the embedment of zero trust capabilities that provide oversight and protection of the user identities that access cloud services and environments. It assumes that no user or device is inherently trusted, even if they operate inside the ICT network. Instead, access to resources is granted on a per-request basis, after verifying the user's identity, and their authorisation to access the resource, limiting the ability to deploy malicious code and undertake attacks that impact supply. Jemena will employ three key identity technology solutions:
  - Cloud Access Security Broker (CASB) – a security solution operating between Jemena users and cloud applications. It provides visibility into cloud usage, enforces security policies, and protects data from unauthorised access.
  - Privileged Account Management (PAM) is a security solution that supports managing and securing privileged (have elevated permissions) accounts and access. Attackers often target these accounts because they can leverage higher levels of access to sensitive data and systems, which provides them with greater capability to be destructive or malicious.
  - Identity and Access Management (IAM) is the process of codifying not only users and groups in a system but also the resources they can access and the functions they

    - can each perform. IAM addresses authentication, authorisation, and access control across ICT systems and ecosystems.
    - The application of password and Secret management will protect sensitive information from unauthorised access. If passwords and secrets are not properly managed, the ICT system can be easily compromised, which could increase the probability of data breaches and security incidents.
- An IoT security model that assumes that no device is inherently trusted will aim to prevent data breaches by encrypting the transfer of data over the internet and within the ICT ecosystem, limiting the ability to operate undetected and applying IoT cyber security standards and tools. It will support mitigating risks associated with security evolution and operational technology through oversight and protection of smarter devices that operate autonomously, are embedded throughout the ICT environment and will become relied upon for rapid fault response and seamless customer experience.
- The ‘detect and protect’ security model focuses on the timely discovery of cyber security anomalies and events by implementing a continuous monitoring capability. In turn, this monitoring capability informs a response function that supports the ability to contain the impact of potential cyber security incidents through automated response or planned intervention strategies. The cyber security ‘detect and protect’ uplift solution will support mitigating security blind spots as ICT environments expand and technologies evolve.
- The cyber security shift left model seeks to embed resources and practices to secure software development through integrated security checks and balances from the beginning of the Systems Development Life Cycle (SDLC) to reduce the risk of vulnerabilities being introduced into the software prior to deployment. This approach will support mitigating risks associated with operating a secure cloud environment and ensuring security tools and practices align with security evolution objectives to limit vulnerabilities, human error and the unintended exposure of data to bad actors.

Benefits

Beyond safeguarding sensitive information and digital assets, robust cyber security measures are pivotal in managing risks inherent in the digital landscape. Cyber security emerges as a linchpin for resilience and continuity, particularly in critical sectors like electricity supply, where any disruption could have cascading effects on customers. By bolstering defences against cyber threats, we not only support the management of cyber security risks but also mitigate the probability of disruptive impacts on the electricity supply chain.

Fortified cyber security measures safeguard the integrity and confidentiality of sensitive operational data, shielding against potential breaches that could compromise Jemena’s critical infrastructure. Additionally, a strong cyber security posture mitigates possible customer data exposure and financial risks associated with data breaches and operational downtime.

Embracing cyber security is an integral component of corporate risk management. It not only supports the imperative of safeguarding critical infrastructure but also advances broader societal objectives, directly aligning with the goals of the Security of Critical Infrastructure (SOCI) Act. By addressing emerging threats, JEN can contribute to national resilience, protect essential services, and uphold public safety, encapsulating the essence of the SOCI Act’s purpose.

By implementing these controls, Jemena’s aims to reduce the risk rating from “high” to “significant” in the current threat environment.

Risks

The cyber security threats are ever-changing in their approach, and we are also seeing a change in societal and government expectations. The main risk is that this program fails to keep up with these changes or is not agile enough to adapt as the threats change.

Costs

JEN's costs for this option is outlined in the table below.

$2024	RY27	RY28	RY29	RY30	RY31
Total Capex					
Non-recurrent Opex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Recurrent-step Opex		[redacted]	[redacted]	[redacted]	[redacted]
Total Opex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Totex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

This is an Enterprise-wide initiative, which means the costs of operating this program are shared across a broader set of Jemena enterprises. A consequence of this approach is that JEN's customers benefit from (i) lower costs and (ii) greater purchasing power when negotiating vendor contracts. [redacted]

Summary

Delivery of cyber security capability will embed cyber controls in step with technology advancement providing fit-for-purpose protection and response in line with cyber security threats, supporting JEN in the safe and reliable operation of the Jemena Electricity Network. This option is recommended as we consider it reflects good industry practice given the benefits and risks outlined above.

Options Summary

The table below summarises the quantitative and qualitative differences between the analysed options.

$2024	Capex	Opex	Totex	NPV	Residual Risk
Option 1	Not applicable	Not applicable	Not applicable	Not applicable	High
Option 2	[redacted]	[redacted]	[redacted]	[redacted]	Significant (refer to attachment A)

What We Are Recommending

Jemena recommends Option 2.[5] [redacted]

We consider Option 2 also reflects good industry practice given the benefits and risks outlined above. Furthermore, it provides the most efficient cost.

Dependencies on other Investment Briefs

Not applicable.

Relationship to ICT Capital Forecast

The supporting modelling for this investment brief is contained in the following framework model: **JEN – IT Investment Brief – Cybersecurity Program – Costs and Benefits Analysis Model.**

[5] This initiative is part of an enterprise-wide approach and was also included in the Jemena Gas Networks (NSW) Ltd. (JGN) Access Arrangement (AA) proposal. The proposed option received approval as part of the AER's 2025-30 Draft Decision.

[redacted]

[redacted]

[redacted]

[redacted]

Attachment B

Jemena Cyber Assurance Framework

[redacted]