Jemena Electricity Networks (Vic) Ltd

Technology Plan

IT Investment Brief - Cyber Security Enhancements

Non-Recurrent - Compliance and Maintain

Glossary

Current regulatory period	The regulatory control period covering 1 Jan 2016 to 31 Dec 2020
Intervening period	The period covering 1 Jan 2021 to 30 Jun 2021 covers the time between the current regulatory period and the next regulatory period. The Intervening period arises with the move from a calendar year regulatory year to financial.
Next regulatory period	The regulatory control period covering 1 Jul 2021 to 30 Jun 2026
RYxx	Regulatory year covering the 12 months to 30 June of year 20xx for years in the Next Regulatory Period and the 12 months to 31 December of year 20xx for years in the Current Regulatory Period *For example, RY19 covers 1 January 2019 to 31 December 2019 and RY22 covers 1 July 2021 to 30 June 2022. For readability, regulatory years during the current period are written in the form CYxx*
CYxx	The calendar year which covers the 12 months to 31 December of year 20xx. For the current regulatory period, this is equivalent to RYxx
JEN	Jemena Electricity Network (Vic) Ltd.
ICT	Information and Communications Technology
Jemena	Refers to the parent company of Jemena Electricity Network

Cybersecurity Non-Recurrent Projects

Objective	The objective of the non-recurrent cybersecurity projects in this document is to ensure Jemena Electricity Network (**JEN**) has a preventative, detective and corrective response to defend the network from cybersecurity threats and attacks while continuing to operate a safe, reliable and efficient energy network. This document covers non-recurrent capital projects for cybersecurity. These are projects individually valued under $1m but in aggregate exceed $1m that enhance or extend JEN's cybersecurity capabilities to meet emerging threats and are for lifecycle updates of systems that occur on a frequency of less than once every five years.
Background	JEN, and its related asset entities, have embraced digitisation and automation. However, automated systems introduce pathways for malicious actors to take control and cause damage, loss of data and financial loss through cyber-attacks. Jemena operates two major distribution networks, JEN and Jemena Gas Network, several gas transmission pipelines and a range of other infrastructure services businesses. These businesses, as well as Jemena's corporate offices, share a single ICT environment. This approach to sharing IT costs and services across a customer base higher than JEN allows all of Jemena's customers to benefit from a lower overall cost, including JEN's customers. Jemena operates a single cybersecurity program to protect the ICT environment and operational technology systems with costs shared between the subsidiaries. Costs are shared based on an apportionment that is standardised across all areas of ICT capex. Cybersecurity is a growing concern for Jemena, the broader business community and Governments. The number of digital devices connected to Jemena's networks is growing rapidly, and traditional, manual business processes are being digitised. This trend, along with global growth in cyber-crime, is driving both the likelihood and consequence of a successful cyber-attack to increase. The increasing number of devices and digital systems increase the number of potential attack vectors for attackers to exploit. Each additional software system increases the possibility of an unknown software flaw being introduced, which also increases the likelihood of an attack being successful. Reliance on digital systems increases the consequence of a cyber-attack as the business will lose functionality. Also, the drive to automation means that spare staff capacity and manual processes are not retained in all cases. This limits the fallback options available to the business in the event access to digital systems is lost, increasing the consequence of an attack. To meet customer expectations for safe and reliable electricity supply and to meet obligations such as the Security of Critical Infrastructure Act[1] regarding cybersecurity JEN must continue to invest in systems to identify, protect, detect, respond and recover from cyber-attacks. This requires non-recurrent investments in new capabilities to ensure cyber defences are upgraded to combat increased sophistication of cyber threats and attackers. JEN also has some security systems that require lifecycle updates that are at a frequency of less than once every five years. These tend to be for significant updates, while minor updates occur at higher frequencies. As the frequency is less than one in five years, these upgrades are also classified as a non-recurrent expenditure.
External Obligations	In 2018, AEMO released the Australian Energy Sector Cyber Security Framework (AESCSF) as a best practice guide for organisations operating in the National Electricity Market. As part of this framework, maturity indicator levels (MIL) were incorporated as a set of graded standards to demonstrate a businesses' cybersecurity capabilities. More recently, updates to the AESCSF framework (version 2019-8) incorporated "Security Profiles" (SP). Based on the AESCSF standards—JEN, which is categorised as 'moderately critical' per the Critical Assessment Tool (CAT) "should achieve" SP-2 level of security (this is akin to the MIL2 standards). JEN considers that meeting the MIL2/SP-2 standard is a prudent approach to ensuring the security of supply and is in keeping with the AESCSF standard to managing the cybersecurity risks our industry faces. JEN has several areas that require improvement to meet MIL2/SP-2. Specifically, the current

[1] Security of Critical Infrastructure Act (Cth. 2018).

	capability to detect and respond to cybersecurity incidents on a 24x7 basis is limited to best efforts by internal staff, with only monitoring by an externally managed security service provider. This approach leaves a significant amount of time where incidents may be detectable, but where no response takes place. In its Non-network ICT capex assessment approach[2] the AER notes that "*Expenditure to achieve a higher cyber security maturity compliance requirement*." qualifies under *Non-recurrent – compliance*.
Customer Importance	ICT is a primary enabler of JEN's ability to operate a safe, reliable and efficient network. Advancements in the areas of big data, mobility and smart networks are quickly transforming how assets and operational processes can be managed. However, these systems also expose businesses to the threat of cyber-attacks. To provide customers with the benefits that ICT brings to the distribution of electricity, the investment must be made in cybersecurity to ensure the ICT systems are robust and reliable. The energy industry, including electricity distribution networks, is particularly exposed in the event of a cyberattack. Some network automation devices, if taken control of remotely by malicious attackers, could disable the supply of electricity, cause damage to equipment and expose the staff and public to safety risks. Spoofing of work orders and instructions to field staff could result in JEN workers unknowingly causing the same result 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 customers in many ways including inaccurate billing, more prolonged outages and increased operating costs. The theft of sensitive customer data could also adversely affect customers and reduce trust in JEN. JEN's priority is to operate a safe and reliable energy network in addition to protecting customer data and information. Cybersecurity investment is critical to ensure these customer objectives can be achieved.
Strategic Approach	To have a fit-for-purpose cybersecurity plan, Jemena is adopting the Australian Signals Directorate's (ASD) *Essential 8* recommendations in addition to elements of the Cybersecurity Framework (CSF) developed by the US National Institute of Standards and Technology (NIST). Aspects of the ASD and NIST standards will be implemented where these standards contribute to a stronger and more robust cyber strategy and where the investment results in an efficient cost outcome for JEN and its customers. The NIST Cybersecurity Framework is a global standard for cybersecurity and protection of critical infrastructure. It has five core objectives: 1. **Identify**: assessing the threats and risks to systems and understand the vulnerabilities 2. **Protect**: defending systems from attack with best practice approaches 3. **Detect**: having tools and protocols in place to spot when a breach has happened 4. **Respond**: reacting quickly using automated safeguards to contain the breach and have protocols in place to mobilise resources 5. **Recover**: having plans in place to handle the aftermath, communicate the outcomes and review the learnings. Jemena's investment in cybersecurity takes guidance from several security-focused organisations in determining the combination of products and services that provide the best and most cost-effective protection. The Jemena cybersecurity systems identify existing areas of network vulnerability as well as opportunities for improvement to ensure currency of the systems. Investment opportunities modelled to specifically address the existing vulnerabilities in the network as well as enhance the cyber responses. An initiative list is maintained and referenced against each focus area to demonstrate how JEN investments in cybersecurity are improving the strength of the cybersecurity program.
Investments	JEN has proposed 18 non-recurrent projects for cybersecurity. We categorise these as either non-recurrent - maintain (four projects) and Non-recurrent - compliance (14 projects), consistent with the approach outlined in the AER latest guidance on assessing ICT expenditure.

[2] AER's Non-network ICT capex assessment approach, Pg 9

Non-recurrent - maintain

JEN has four non-recurrent lifecycle projects planned for the next regulatory period. The annual expenditure on each of these projects is shown in the table below.

Direct Escalated Costs (mid-year $2021)

Project Title ($2021)	Project ID	RY22	RY23	RY24	RY25	RY26
Active Directory Migration (cloud)	ITSE21			89,501	89,837	
Certificate Services Migration	ITSE24		82,309	82,616		
Identity Access Management Migration	ITSE31	177,701	178,335	89,501		
SIEM (Corporate Zone) Replacement	ITSE40			268,502	269,512	
Total		**177,701**	**260,644**	**530,120**	**359,350**	**0**

Total expenditure on these *non-recurrent – maintain* projects during the next regulatory period is $1.3m

These projects are required to retain existing capabilities and tend to be recurrent but with frequencies of less than once every five years.

In the cases of the following projects, JEN is either planning to move to a new product or shift an existing system to a cloud solution rather than perform in-place lifecycle upgrades:

- **Microsoft Active Directory** – vendor product roadmap proposes a shift to the cloud in the planning horizon. Based on experience with the current approach and the likely scope, Jemena estimates this to be a small to medium-sized project completed in less than 12 months with medium complexity.
- **Certificate Services Migration** – market analysis is suggesting this may be better handled as a cloud solution as the number of certificates and breadth of providers grows. Based on experience with current approaches and the likely scope, Jemena estimates this to be a small to medium-sized project to be completed in less than 9 months with medium complexity.
- **Identity Access Management** – market analysis suggests that more feature-rich approaches from other service providers will serve Jemena's needs better and we expect to migrate to a new mechanism for authenticating users from the beginning of the period. Based on experience with current approaches and the likely scope and the breadth of systems requiring authentication services, Jemena estimates this to be a three-staged project with each being a small to medium-sized project completed within 12 months and with medium complexity.
- **SIEM** – Jemena's Security Information & Event Management (SIEM) tool draws data about security events from the other security products in the environment and analyses and logs them. It is currently handling as many as 500 million such events each week. As the level of automated cyber-attacks rises, and the number of security products in use across Jemena expands, this puts pressure on the SIEM tool to handle the workload. Jemena's ability to detect and respond effectively through analysis of the security logs is key to maintaining defences, and it is anticipated that new products with higher throughput and better real-time analysis features will become available and will need to be adopted. While the precise nature of the solution is yet to be determined, experience with the current system and our anticipation of the volume growth has informed Jemena's estimate of a large project to be completed in less than 12 months with medium complexity.

Compliance Enhancements

JEN has 14 enhancement projects, most of which are relatively small. These have been classified as non-recurrent – compliance as they seek to maintain the current risk profile as threats increase and thereby maintain current service levels. The annual expenditure on each of these projects is shown in the table below.

Project Title ($2021)	Project ID	RY22	RY23	RY24	RY25	RY26
Application Whitelisting	ITSE22	68,916			69,682	
Automatic Vulnerability Management Scanning	ITSE23		62,875			
Cloud Access Security Broker (CASB)	ITSE25		75,450			
Container Security	ITSE26	75,181			76,016	
Information Rights Management/Data Loss Prevention	ITSE27	34,173	34,295	34,423	34,553	34,683
Endpoint Detection & Response	ITSE28	137,832			139,363	
Establish Dark Disaster Recovery Capability	ITSE29	28,478	28,579	28,686		
Intrusion Detection/Prevention Uplift	ITSE32		150,899			
IOT Security Capability	ITSE33	207,317	104,029			
Network Segmentation & Access Control Review & Uplift (IT/OT)	ITSE34	31,325	31,437	31,555	31,673	31,793
Multi Factor Authentication (MFA) (IT/OT)	ITSE35	150,362				
Perimeter Security Uplift (Cloud Firewalls, Secure Web Gateway)	ITSE37		150,899		152,033	
Remote Access Controls (Support, 3rd parties, Partners, etc. for FIRB/CIC)	ITSE38			69,420		
Web-Based Attack (DDoS) Prevention	ITSE41				69,682	
Total		**733,584**	**638,464**	**164,085**	**573,002**	**66,476**

Total expenditure on these *non-recurrent – compliance* projects during the next regulatory period is $2.2m. The total for all the Non-recurrent projects is $3.5m

These projects are deployed to ensure JEN's cybersecurity capabilities keep up with the increasing capabilities of cyber attackers. JEN does not expect that these projects will result in an increase in security, due to the rapid evolution of threats, but to be keeping pace with the threats and maintaining the current risk exposure.

Some projects, such as IoT Security Capability, are required to extend the existing security capabilities to new products and devices that will be connected to JEN's network during the next regulatory period.

More detailed descriptions of enhancement projects are below:

- **Application whitelisting** will be a new product or service which will specify an index of approved software applications that can be present and active across the IT network and enforce the restriction. Application Whitelisting is among the ASD's *Essential 8* list of security mitigations and one which is a priority for Jemena to address.
- **Automatic Vulnerability Scanning** will be a new product/service which will scan for known vulnerabilities in Jemena's systems so they can be proactively remediated. It speaks to the theme of automated *Detect* and *Respond*.

	• **Cloud Access Security Broker** will be a new product/service to monitor the use of cloud services and allow Jemena to apply security policies to them. This will provide additional capabilities to *Protect* systems through the application of security policies, *detect* malicious traffic through monitoring and *Respond* to cybersecurity breaches through the application of security policies. • **Container security** will provide Jemena with the ability to secure the integrity and confidentiality of applications that operate in virtual and cloud native environments. This will provide additional capabilities to *Protect* cloud applications from security threats. • **Information Rights Management/Data Loss Prevention** will be a new product/service to prevent important information from leaving the control of Jemena and detect if such information does leave Jemena's control. This will provide additional capabilities to *Protect* data and *Detect* cybersecurity breaches. • **Endpoint Detection & Response** will be a new product/service to *Protect* end-user devices from being attacked through malicious code, such as viruses. • The **Dark Disaster Recovery** (**DR**) initiative will provide some protection from the growing threat posed by crypto-locking malware by ensuring that there is an available option to revert to a previous known good state if all our systems, on-line DR and backups are compromised at once. This will provide additional capabilities to *Recover* from attacks. • **Intrusion Detection/Prevention Uplift** will be a new product/service that will look for anomalies on the network that indicates an attack in progress. This will provide additional capabilities to *Detect* attacks. • **IoT Security Capability** will be a new product/service to provide security controls for the increasing number of Internet of Things devices that are expected to be connected to the JEN network over time. This will provide additional capabilities to *Protect* these devices. • **Network Segmentation** will be a new product or service that will permit limits to be placed on which elements of our network can interact with others. This could prevent, for example, an infected laptop passing malware onto other equipment that it would otherwise not need to interact with. • **Multi-Factor Authentication (MFA)** will improve Jemena's ability to verify a computer or a person connecting to the communications network. This project will strengthen our MFA from devices and users to help *protect* our systems from being accessed by unauthorised systems or people • **Perimeter Security Uplift** will lifecycle existing products with modern equivalents to *Protect* our boundaries from unwanted system communications • **Remote Access Controls** will be a new product or service that will provide the ability to have context-aware remote access. This will prevent staff from accessing some elements when travelling overseas and is a Foreign Investment Review Board requirement for some assets. This will provide additional capabilities to *protect* sensitive data and systems. • **Web-Based Attack (DDoS**) **Prevention** will be a new product or service to minimise the impacts of these attacks on our many public-facing services such as our customer portals. DDoS attacks now occur daily on Jemena's external services. This will provide additional capabilities to *Detect* and *Respond* to security threats. Implementing these new defences, configuring them and monitoring them will require additional resources. To allow for this, JEN has proposed an opex step change. This is detailed in the document "*Att 06-05 Operating Expenditure Step Changes – 020200131 – Confidential*".
Benefits	The proposed projects would not increase security, and therefore benefits, relative to the current security level. Unlike traditional network investments, cybersecurity requires enhancement overtime to maintain security levels. This is because cybersecurity threats and attackers are also becoming more sophisticated over time. The benefit of these projects is that security levels will not fall.

Risks	There are no material risks associated with the deployment of these projects. However, not implementing these projects is likely to have material consequences over the next regulatory period, as the cyber risk escalates at an exponential rate.
Relationship to ICT Capital Forecast	The proposed projects are contained in the ICT investment plan as 14 separate non-recurrent projects. These are Non-recurrent – maintain Project IDs: ITSE21, ITSE24, ITSE31, ITSE40 and Non-recurrent – compliance Project IDs: ITSE22-23, ITSE25-29, ITSE32-35, ITSE37-38 and ITSE41 (Non-recurrent – compliance).