

Information Technology Focussed Conversation

1. Recommended Service Outcome/ Investment Option

Workshop participants are recommending to the People's Panel that SA Power Networks should invest to support Cyber Security capability Option 2 – Maintain.

The IT Focussed Conversation did not seek endorsement of the whole IT investment program. In addition to reviewing the cyber security capability requirement, it was to inform participants of the investment needed to maintain existing IT services, and to highlight the specific IT funding required to support/enable initiatives recommended from the other Focussed Conversation topics.

2. Recommended Option: Cyber Security Option 2 - Compliance

Option 2 provides for the investment level required to enable achievement and maintenance of the AESCSF (Australian Energy Sector Cyber Security Framework) Security Profile 3 (SP3).

Outcomes of this Option for customers include:

- alignment to legislative requirements anticipated to be required by the end of 2030;
- improvement in system resilience, with systems more quickly returning to operational as people are more prepared and processes are better;
- systems required to operate the network are better trusted and more able to be relied upon by operators, supporting the continual delivery of services;
- reduced risk of a cyber security incident that delays the delivery of a service or resolution of an outage; and
- more secure digital experiences for customers with SA Power Networks across a broader range of online services, with greater protections over customer confidential information.

3. Why are we recommending this option?

Workshop participants recommended Cyber Security Option 2 – compliance over the other options because they felt that:

- meeting expected legislative requirements is a clear and given requirement; and
- in the absence of independent expert opinion, meeting ASECSF SP3 should enable the business to address an adequate level of cyber security risk.

While stakeholders considered the benefits associated with additional investment in cyber security above expected legislative requirements, the consensus was to endorse a more prudent investment level.

4. The high-level impact on the customer’s bill of this investment option

The estimated costs for the 2025-30 period for the increased investment in cyber security are:

- Annual Cost \$7.3 Million
- Total 5 year cost \$36.5 Million

This proposed uplift represents an increase to approximately double what SAPN is currently spending on cyber security.

Indicative bill impacts for residential and business customers for the 2025-30 period for cyber security are:

	Residential (average \$ annual)	Business (average \$ annual)
Option 2 - Maintain	\$5.25	\$40.85
Total distribution bill	\$505-\$590	\$3,950-\$4,650

It should be noted that these forecasts are based on the Iteration 2 scenario and are in \$2022. IT forecasts will be refined by SAPN’s Regulation team over the coming months into a forecast Iteration 3, and will be adjusted to reflect both conversion to \$2025 and the RBA’s revised inflation forecast.

5. Why the other options were not supported and have not been recommended

Option	Rationale of why not supported
Option 1: Basic (as is)	- Stakeholders were cognisant of the evolving threat landscape and considered that continuation of the existing level of investment would not provide the ability for SA Power Networks to meet the ever-increasing cyber security threat - Stakeholders recognised the requirement for SA Power Networks to meet expected legislative obligations, and endorsed the SA Power Networks opinion that this was likely to require meeting AESCSF SP3 by 2030
Option 3: New Value (Advanced)	- Stakeholders generally believed that SA Power Networks should not have a mandate to exceed expected legislative requirements (AESCSF SP3) - While stakeholders were cognisant of the relatively modest increase in the cost of option 3 relative to option 2, they considered that the accumulation of these 'additional' costs were adding to a total investment level that would place too great a burden on customers.

6. Areas of contention, key discussion points or concern

In arriving at the recommendation, the Focussed Conversation explored the following key questions, contentious issues and divergent views:

Discussion Area	Comment / Concern
Compliance obligations	- AESCSF SP1 has been drafted into legislation and is expected to be enacted within the next 18 months - This recommendation assumes that AESCSF SP3 will be legislated prior to 2030 and hence will become the new minimum requirements for compliance during the 2025-30 Regulatory Control Period - Cyber security risks are increasing, not decreasing, and specific regulations may be imposed by legislation / the Australian Energy Regulator (AER) regardless of the group's opinions
IT as an enabler / IT forecasts	- IT is an enabler of the business. The total proposed IT investment (Forecast Iteration 2) is \$410.9 million. This includes Scenario 1: IT Basic (\$217.3 million), Scenario 2: IT Maintain (\$112.6) and Scenario 3: New Value (\$81.1 million) and reflects capex plus new (incremental) opex. - The Cyber Security capability uplift is part of Scenario2: Maintain. Other than this item, Scenarios 1 and 2 were presented for information only. This IT expenditure will be assessed and benchmarked by the AER against their ICT evaluation criteria to determine whether it is prudent and efficient. - Scenario 3 – New Value IT costs are the IT component of delivering the preferred scenario from the other Focussed Conversation workshops, which we are required to highlight and describe separately within the IT submission (hence it is not a duplication of the costs). The IT Focussed Conversation was deliberately held at the end of other workshops, so a summation of the IT costs of the New Value items from those workshops could be provided. For example, this includes \$37 million in IT costs to support the Reliability & Bushfire Safety program (2.7% of the total Reliability & Bushfire program). - If any of these other Focussed Conversation scenarios are not progressed, the related New Value IT expenditure will be removed. Non-acceptance of the IT costs for these proposed business programs would result in SA Power Networks not being able to deliver the programs.

Discussion Area	Comment / Concern
	- IT capex will be recovered over a five year period from when it is spent. Opex is generally recurrent expenditure and will be funded from a total annual opex allowance approved by the AER. The majority of expenditure will therefore be recovered in the 2025-30 year period and the remainder in following regulatory period. - The AER has already accepted the need to move to AESCSF SP3 for similar businesses (e.g., ElectraNet). SA Power Networks could therefore likely not recover cyber security uplift as a pass-through event and needs to forecast this in its proposal.
Complexity of topic being discussed	- It was noted that this is a complex and specialised area and it therefore may be beyond the ability of people in the room to assess adequately. - Community Advisory Board (CAB) is relying on the AER to ensure the proposal is prudent and efficient to enable achievement of AESCSF SP3. - Participants discussed the speed of change in the area of cyber security and the rising level of risks and the importance of being prepared rather than playing catch-up.
Acceptance of Risk	- The greatest risk for SA Power Networks associated with cyber security is the risk to the security of the network and the resulting disruption to electricity supply - The SA Power Networks Board could choose to invest additional amounts if it is unwilling to accept the level of risk that funding will mitigate
Options and recommendation	- Participants noted the significant additional cost from Option 2 compared with Option 1, though also noting the additional benefits - One participant questioned the basis for moving to Option 3 if SA Power Networks currently has good defences and no reportable offences - One participant supported Option 3 due to the relatively small incremental cost for the additional value provided; and the potential for this functionality to cost more if left until future years

7. The People’s Panel may choose to interview key staff, stakeholders, or subject matter experts from the Focussed Conversation or request to speak to the Peoples Panel in 2023

Name	Position / Organisation	What the person can speak about
Dan Popping	Head of Stakeholder Engagement, SA Power Networks	Co-author of this document
Nathan Morelli	SA Power Networks, Head of Cyber Security and IT Resilience	- SA Power Networks Cyber Security Strategy - SA Power Networks 2025-30 cyber security options and costings - Global cyber security environment
Matthew Pritchard	SA Power Networks, Head of IT Strategy	- SA Power Networks IT Reset Strategy - SA Power Networks IT Expenditure forecasts
Kelvin Trimper	Chair CAB Reset Subcommittee	- Workshop information presented and outcomes - Customer engagement and process

8. The following external stakeholders were part of the Focussed Conversation

Name	Position / Organisation	Workshop 1
Dr. Jessie Byrne	Chair, Community Advisory Board	✓
Kelvin Trimper, AM	Deputy Chair, Community Advisory Board	✓
Andrew Stock	Customer Advocate, Community Advisory Board	
Michael Leane	Customer Representative, Community Advisory Board	✓
Davis Veremu	Multicultural Representative, Community Advisory Board	✓
Doug Strain	Customer Representative, Community Advisory Board	
Georgie Morris	Customer Advocate, Community Advisory Board	✓
Chris Marsden	Reset Subcommittee	✓
Jordan Smith	Business representative, Reset Subcommittee	✓
Mark Henley	AER CCP30	
Mike Swanson	AER CCP30	✓
Slavko Jovanoski (partial attendance)	AER	✓