Cyber security efficient costs

Revised Regulatory Proposal 2024-29

30 November 2023

PowerWater

Contents

List of tables

List of figures

1. Background

In this document, we propose prudent and efficient opex step changes consistent with the objectives and criteria in the NT NER.

All dollar values in this Attachment are in real 2024 terms unless otherwise stated.

1.1 Our Initial Regulatory Proposal

In response to heightened cyber security and critical infrastructure concerns the Federal Government recently introduced new legislative obligations to ensure the physical and electronic security of Australia's critical infrastructure. This includes electricity networks. We are now required to increase our cyber security capability significantly to achieve and maintain the necessary practices and anti-patterns.

In response to heightened cyber security and critical infrastructure concerns, in 2018 the Federal Government passed the Security of Critical Infrastructure (SOCI) Act, which introduced obligations in the electricity, gas, water and ports sectors to ensure the physical and electronic security of Australia's critical infrastructure.

Based on the Electricity Category (E-CAT) rating in the AESCSF, Power and Water is a participant of Medium Criticality and a Security Profile 2 (SP-2) level of cyber security reliability is recommended.

Based on other electricity utilities' plans and its own discussions with the AER and the NT government, and cognisant of recent cyber security attacks on Australian telecommunications, electricity retail, and health sectors, we consider that achieving and sustaining SP-2 under the AESCSF as quickly as practicable is prudent.

As recommended in the AESCSF, we will prioritise delivery of the 'Priority Set' practices for SP-1 and SP-2 For prudence and efficiency, we intend, where practical, to limit practices to the specific assets and services required under the legislation or to meet foreseeable, material and/or emergent risks. Other frameworks and standards that offer guidance on how to implement these elements will also be used and aligned to AESCSF.

Our recommended option includes prudent selection of technology, process and information-based initiatives to enable us to improve priority capabilities efficiently and incrementally (and in groups/phases) on a risk-prioritised basis. The estimated total cost of this option is $31.4 million (totex) across Information Communication and Technology (ICT) and Operating Technology (OT) to which $12.9 million is opex and, $18.4 million is capex.

This is the recommended option, as it is the only viable option which:

- Affords the flexibility to address the reality of emergent risks.
- Addresses the resourcing challenges in the Territory.
- Provides certainty and manageability of delivery.

This option ensures coverage of ICT and OT to incrementally establish, operate, mature and sustain SP-2 compliant levels of performance.

For the next Regulatory Control Period (RCP), the business case included $11.4 million capex and a further $4.4 million[1] was allocated to Standard Control Services (SCS). This supports achievement of SP-2 by the end of the 2024–29 regulatory period

The cost estimates were derived from a combination of vendor, consultant, and subject matter expert advice based on a detailed gap analysis.

More information on this program of work (capex and opex) was provided in the Business Case: Cyber Security baseline (see Attachment 8.72 included with the IRP).

1.2 AER's draft determination

In its draft determination, the AER accepted our proposed capex forecast and operating expenditure step change for the next regulatory period. The AER noted this was accepted as a placeholder, being subject to additional information being provided in our RRP to justify that these are efficient costs.

The AER accepted the scope of our cyber security project and the nature of the investment for each initiative to deliver SP-2 compliance is prudent. The AER provided guidance on the further information to be included in our RRP to confirm the basis of our proposed costs, and which we have included in this Attachment. This included:

- Description of the proposed actions to address each of the maturity/capability gaps it identified between its current level of cyber maturity and the level required to achieve SP-2 maturity across each of the 11 domains under the AESCSF framework.
- Linking each of the above proposed actions to the respective individual costs required to undertake these actions.
- Detail for the individual costs inputs related to each proposed action, the basis for these costs (including relevant inputs, calculations, assumptions and sources) and set out how they were estimated, such as the number of labour-days or license fee.
- Demonstrating the efficiency of each cost input, through market testing and detailing all assumptions or other independent expert reports.

[1] After submission, we identified a transcription error between the information included in the business case and that included in for the opex step change

2. Revised Regulatory Proposal

Power and Water's RRP focusses on additional information requested by the AER. We provide a table of our response to the specific requests that we have received for the cyber security project in Appendix A.

2.1 Response to draft determination

Power and Water's RRP is aligned with the information submitted as a part of our Initial Regulatory Proposal (IRP), corrected for a transcription error in the opex step change. This information should be read in conjunction with the business case submitted with our IRP for cyber security.

We provide this supplementary submission to describe the process we have undertaken to develop our cost estimates, the procurement process that we are undertaking to secure the required services that includes market tested processes, and updated information that confirm the efficiency of our cost estimates where market tested processes are not available.

2.2 Identification of business need

2.2.1 AER has supported the need for this expenditure, and assessment of the scope of the project

Power and Water's cyber security maturity is not adequate to comply with the obligations under the amended Critical Infrastructure Act nor robust enough in the face of the worsening cyber-attack landscape. This business case supports achievement of SP-2 (per the Australian Energy Sector Cyber Security Framework, 'AESCSF') by the end of the 2024-29 regulatory control period ('the next RCP').

Power and Water is proactively managing it cyber security risk and compliance to the Security of Critical Infrastructure (SoCI). The SP-2 of the Australian Energy Sector Cyber Security Framework, 'AESCSF' has been approved by the Power and Water Board and the target state and one which also meet compliance against SoCI legislation.

The AER accepted the scope of our cyber security project and the nature of the investment for each initiative to deliver SP-2 compliance is prudent.

2.2.2 Power and Water has undertaken extensive assessment

Power and Water has included a cyber security function in its Corporate and Operational Technology business units. This has included a number of permanent and contracted positions to support the business from an operational perspective. As Power and Water have selected the blend of internal and external resourcing to achieve the required security level.

The cyber security project follows an extensive assessment of the requirements to manage the assessed cyber security risks.

The AER accepted the scope of our cyber security project and the nature of the investment for each initiative to deliver SP-2 compliance is prudent.

2.3 Selection of the efficient option

2.3.1 Determination of initial estimate

Power and Water has used the rates below to determine the cost estimate, and which produces an average rate of $1,500 per day. These rates are applied to our BAU budgeting process:

- Internal Resource - [redacted]
- Cyber Security Analyst - [redacted]
- Cyber Security Analyst - [redacted]

The initiative sequencing and estimated effort was then multiplied by the average rate of $1,500 per day to determine the estimated cost of the initiative. These estimates were used for the submission as included in the ICT Cyber security baseline business case (8.72 RBC ICT Cyber Security Baseline – 31 Jan 23). All costs are confirmed using the Power and Water governance for business case and procurement processes.

In some cases, the procurement phase has commenced and in other cases already completed. In section 3 we have referred to proposals, contracts and invoices as evidence of the costs that we have and expect to incur. Where we have actual cost information, we have found that this aligns well to our initial estimates which provides confidence that initial estimates are reasonable.

The cost estimates included for opex also include the running of the cyber day-to-day operational practices as they form the processes and practices that are needed to achieve compliance. These resources will be involved as secretariat for the Power and Water Security Council or for the purposes of reviewing and updating or approving configuration changes for security enhancements.

Following the development of the business case, we engaged assistance from Ernst and Young to undertake a health check of all ICT regulatory business cases. In general, the health check found that our proposed expenditure for the next RCP was comparable to other network service providers.

As noted above, the outcomes of our procurement processes for cyber security packages indicates that contracted costs are within reasonable bounds of our initial estimates.

Power and Water has been engaging with the Australian Cyber Security and Department of Home Affairs to ensure that the programs continue to align with the expectations of the Department.

2.3.2 Application of our procurement framework and process to external costs

The Power and Water procurement framework is both a rigid and fair process that is undertaken to ensure that potential proponents have an opportunity to put their proposals forward.

We are committed to our key procurement principles, these principles must be applied to every procurement activity, regardless of value and complexity of the procurement activity.

- **Open competition** - no unwarranted barriers to the participation of potential suppliers. Best value for Territory is best achieved if there is competition between a range of potential suppliers
- **An informed Buyer** - Power and Water buyers and procurement practitioners have accurate information about the supplier market, and are open to the potential for different products and market approach models to meet Power and Water's needs

- **Fair and objective tender and evaluation processes** - the assessment of suppliers' responses is based on fair and objective assessment criteria and analysis that recognises enhancement of industry and business capabilities in the Northern Territory.

The process applied to the cyber security work packages was an open competitive process, which means the following process was undertaken:

1. A Future Tender Opportunity released for a period of time.
2. A procurement plan developed and approved by appropriate delegate.
3. In conjunction with the allocated procurement partner, develop and, ensure that all quality assurance checks are completed for the request for tender (RFT) documents, prior to the RFT documents being sent to multiple selected vendors as part of the open competitive tender process.

Power and Water has established a number of key partnerships with suppliers such as, [redacted]

In addition to above partnerships, Power and Water has established a panel to utilise external capacity and capability from cyber security experts, and by utilising an insourced and outsourced model of staff and contractors. The cyber security contractors that have been engaged to date, have been assisting Power and Water to manage potential threats and, as mentioned above building the capability of internal staff so that in future years we will eventually have the required skillsets to manage the growing threats that may attack our infrastructure and customers'.

2.3.3 Adoption of rigorous project management controls

The cyber security work packages are or will be being bundled together to follow the Project Investment Delivery Framework (PIDF), which is governed by our Enterprise Portfolio Management Office. Projects and Initiatives such as above are reported and monitored through Power and Water Board and Management Committees.

PRINCE2 methodology is used to assist in the project management of the ICT Portfolio. This process based approach means projects are thought about from an end to end process, therefore meaning that each stage of the project is considered in depth and detail, with clear and concise precision, finally the project follows a post implementation review meaning that the project is neatly concluded.

As with all projects there are strict processes that are placed on both timing and cost controls. Specifically to the ICT Portfolio, projects are reported back through Power and Water Board and management committees. To reduce the likelihood of cost overruns, there will be cyber security steering committees established and a Security Council has been established to monitor the importance of dealings with the Power and Water Cyber Security Program.

Finally, given the importance and value of our infrastructure and customer details, as part of our contractor performance for our external contractors and parties, we include penalty rates for the overrun or the non-delivery of services or support.

2.3.4 Our program for cyber security continues to have strong consumer support

As a part of our regulatory process, we tested our ICT expenditure with residential customers at our People's Panels (Panel) in May, August and October 2023.

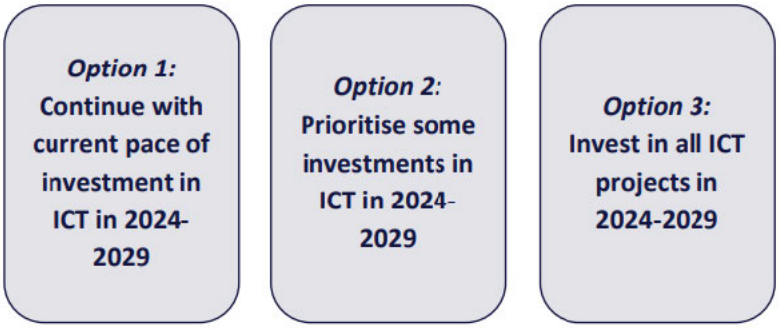
In May we explained to the Panel how our ICT infrastructure is changing. We completed an exercise to demonstrate the changing technologies and discussed the Medibank Cyber Attack to help customers understand why our systems and people need the capabilities to prevent similar attacks on Power and Water infrastructure.

The 3 areas that Panellists were asked to consider were:

- Cyber security to protect customer data and prevent the network being compromised by cyber attack.
- Information technology relating to corporate and administrative systems that help to support business practices and align with relevant regulations.
- Operating technology relating to network operations to allow visibility of the network and asset management.

Figure 2.1 shows the options that the Panel was asked to consider.

Figure 2.1: Options presented to Peoples Panel



Most panellists were largely supportive of Option 2 to prioritise some of the projects or Option 3 to fast-track investment now to improve future service delivery and reduce potential issues and costs. Most Panel members struggled to prioritise one investment over another, expressing the view that all 3 investments are equally important.

In August we held an online session with our Panels at which we continued the conversation reminding Panellists that our ICT systems are 20 years old and no longer vendor supported. Panellists provided the following feedback:

- Improvement and oversight of ICT systems should be a continuous program.
- Power and Water need to have redundancies in the event of disaster.
- More details should be provided around the security of customer information.
- Strong cyber security measures are important and should be regularly reviewed.

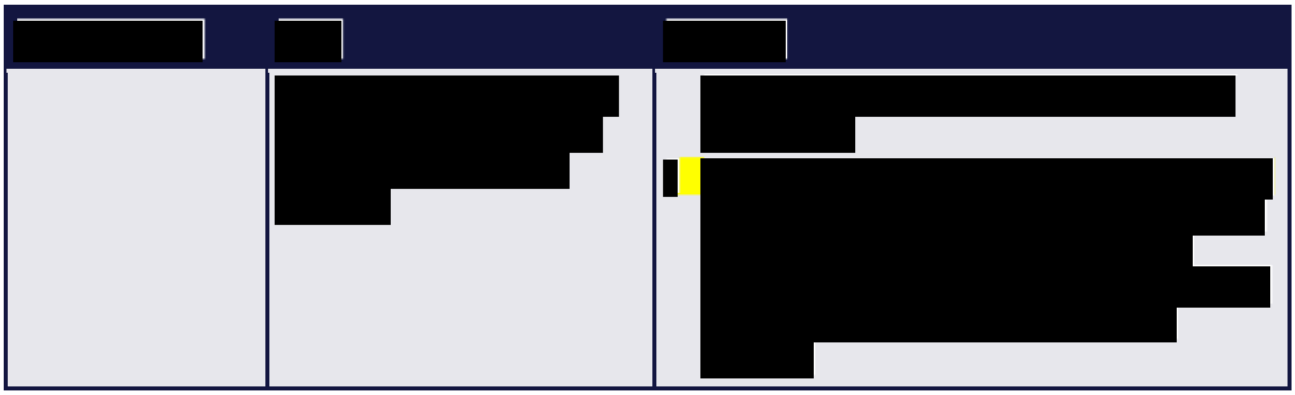
Finally, when we met with our Panel in October, Panellists were asked if they agreed with the refined scopes for our Operating Technology Uplift, Cloud Migration and Cyber Security programs. The Panel showed strong support for these investments and recognised the benefits to both Power and Water and customers such as faster outage and issue response rate, greater security of information and cost savings from migrating to cloud storage.

2.4 Basis of forecast expenditure

2.4.1 Scope of proposed initiatives

Table 2.1 indicates what has been included in the management of the SP-2 requirements.

Table 2.1: Initiative inclusions



2.4.2 Summary of included costs

The list of initiatives require a combination of capex and opex investments. The opex items include ensuring that the systems and processes developed by Power and Water remain current (e.g. third party access improvements once built will have to be maintained). In other cases, Power and Water may not operate or own the asset as has been the case with recent cloud services acquired.

As described in the ICT Cyber security baseline business case (8.72 RBC ICT Cyber Security Baseline – 31 Jan 23), each practice, anti-pattern and domain to achieve SP–2 has been linked to the initiatives listed in Table 2.2, with the associated expenditure in the next RCP.

Table 2.2: Cyber initiatives

Initiative Name	Primary Security Alignment Goal	Next RCP capex ('000)	Next RCP opex ('000)	Evidence Explanation of Costing
CSU-01 Cyber Training Uplift	Create culture of security	[redacted]	[redacted]	Invoices - Cyber CX
CSU-02 Improve security governance	Improve security governance		[redacted]	Invoices - Contractor
CSU-03 Identity and Access Management	Create culture of security	[redacted]	[redacted]	Market based cost (supplier proposal)
CSU-04 Network Access Control Implementation	Secure the Infrastructure	[redacted]	[redacted]	Internal estimate
CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	[redacted]	[redacted]	Internal estimate
CSU-06 Information Security Roadmap	Manage compliance obligations	[redacted]	[redacted]	Market based cost (supplier proposal)
CSU-07 Asset Management	Secure the Infrastructure	[redacted]	[redacted]	Internal estimate

Initiative Name	Primary Security Alignment Goal	Next RCP capex ('000)	Next RCP opex ('000)	Evidence Explanation of Costing
CSU-08 Security Compliance and Governance regulations	Manage compliance obligations		[redacted]	Internal estimate
CSU-09 Data Sharing & Privacy	Protect data	[redacted]	[redacted]	Combination of Market based cost (supplier proposal) and internal estimate
CSU-10 Incident Response Capability	Protect Data	[redacted]	[redacted]	Combination of invoice and internal estimate
CSU-11 Endpoint Security Platform	Compliance obligations	[redacted]	[redacted]	Internal estimate
CSU-12 OT Security Architecture Re-design/Uplift	Secure the Infrastructure		[redacted]	Internal operating cost
CSU-13 Application Security Management	Secure the Infrastructure	[redacted]	[redacted]	Internal estimate
CSU-14 Centralised Logging & Threat Management	Detect & Respond to Threats	[redacted]	[redacted]	Invoices-Dragos, Cyber CX
CSU-15 Forensic investigation tooling to support incident response	Detect & Respond to Threats	[redacted]	[redacted]	Invoices- Dragos
CSU-16 Protection of Backups and Archives	Secure the Infrastructure	[redacted]	[redacted]	Internal estimate
CSU-17 Security Metrics	Manage Compliance Obligations		[redacted]	Internal estimate
CSU-18 Business Impact Assessment Reviews	Manage Compliance Obligations	[redacted]	[redacted]	Internal operating cost
Total		[redacted]	[redacted]	

3. Summary of proposed expenditure

The table below sets out the proposed expenditure for the cyber security program, that aligns with the business case. The basis for the cost estimate and evidence of the actual costs being incurred by Power and Water is described below.

Table 3.1: Proposed expenditure, $million FY22

	2024-25	2025-26	2026-27	2027-28	2028-29	Total
Capex	2.5	3.0	3.0	2.5	2.0	**13.0**
Opex	1.8	2.1	2.1	1.8	1.4	**9.1**
Total	**4.3**	**5.1**	**5.1**	**4.3**	**3.4**	**22.1**

Minor differences may be present due to changing inflation assumptions between the IRP and RRP submissions when the values are expressed in FY24 terms.

3.1 Basis of cost estimate

The initial estimate was determined by internal subject matter experts as included in the ICT Cyber security baseline business case (8.72 RBC ICT Cyber Security Baseline – 31 Jan 23). All values are presented in FY22 terms, as this was the basis in which the business case was developed.

As noted in section 2, all initial estimates were based on a resource estimate using an average day rate of $1,500 per day. We have been progressively securing the services required for these elements via competitive tender processes and found that our estimated hours/days for each of the work packages and our assumed rates are arriving at costs that approximate our estimates.

Where available, we have included further evidence to support our cost estimates.

Table 3.2: Cyber security opex step change, $million FY22

Initiative name	CAPEX Resource estimate based on average rate (days)	CAPEX Estimate $000s (FY22)	OPEX Resource estimate based on average rate (days)	OPEX Estimate $000s (FY22)	Supporting evidence
CSU-01 Cyber Training Uplift	100	[redacted]	100	[redacted]	
CSU-02 Improve security governance	-		50	[redacted]	

Initiative name	CAPEX Resource estimate based on average rate (days)	CAPEX Estimate $000s (FY22)	OPEX Resource estimate based on average rate (days)	OPEX Estimate $000s (FY22)	Supporting evidence
CSU-03 Identity and Access Management	1,067	[redacted]	267	[redacted]	
CSU-04 Network Access Control Implementation	267	[redacted]	300	[redacted]	
CSU-05 ICT Domain Network Segmentation	467	[redacted]	300	[redacted]	
CSU-06 Information Security Roadmap	100	[redacted]	97	[redacted]	
CSU-07 Asset Management	400	[redacted]	333	[redacted]	
CSU-08 Security Compliance and Governance regulations	-		387	[redacted]	
CSU-09 Data Sharing & Privacy	733	[redacted]	300	[redacted]	

Initiative name	CAPEX Resource estimate based on average rate (days)	CAPEX Estimate $000s (FY22)	OPEX Resource estimate based on average rate (days)	OPEX Estimate $000s (FY22)	Supporting evidence
CSU-10 Incident Response Capability	667		1,433		
CSU-11 Endpoint Security Platform	1,000		667		
CSU-12 OT Security Architecture Re-design/Uplift	-		167		
CSU-13 Application Security Management	233		167		
CSU-14 Centralised Logging & Threat Management	667		383		
CSU-15 Forensic investigation	1,000		467		

Initiative name	CAPEX Resource estimate based on average rate (days)	CAPEX Estimate $000s (FY22)	OPEX Resource estimate based on average rate (days)	OPEX Estimate $000s (FY22)	Supporting evidence
tooling to support incident response					
CSU-16 Protection of Backups and Archives	1,667	[redacted]	400	[redacted]	
CSU-17 Security Metrics	-		133	[redacted]	
CSU-18 Business Impact Assessment Reviews	300	[redacted]	117	[redacted]	
Total		13,000		9,100	

3.2 Supporting evidence

The following attachments provide further supporting evidence of the costs that are being incurred and that have been relied upon to determine the efficient level of cost.

Table 3.3: List of supporting evidence

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	
[redacted]	[redacted]	

3.3 Revision to the opex step change included in the RRP

Following submission of our IRP, we identified a transcription error in the proposed opex step change that did not align with the submitted business case. The variance resulting from this error is summarised in the following table.

Table 3.4: Proposed operating expenditure, $million FY22

	2024-25	2025-26	2026-27	2027-28	2028-29	Total
Opex included in the business case submitted with the IRP	1.8	2.1	2.1	1.8	1.4	9.1
Opex included in the opex step change submitted with the IRP	1.4	1.7	1.7	1.7	1.7	8.1
Variation to business case	0.4	0.4	0.4	0.1	-0.3	1.0

When updating the submission for the RRP, the expenditure was averaged over the five year period, without change to the total expenditure included in the business case. The net result is an increase of $0.6 million over the five years after allocation to Standard Control Services (SCS) when compared with the IRP of $4.4 million.

Table 3.5: Proposed opex step change, $million

	2024-25	2025-26	2026-27	2027-28	2028-29	Total
Total Opex relied upon for opex step change (FY22)	1.8	1.8	1.8	1.8	1.8	9.1
Allocation to SCS (FY22)	0.9	0.9	0.9	0.9	0.9	4.5
Allocation to SCS (FY24)	1.0	1.0	1.0	1.0	1.0	5.0

Appendix A

Response to AER questions

PowerWater

Table A.1: Information requested by the AER in the draft determination

Information requested by the AER	How we have responded
Description of the proposed actions to address each of the maturity/capability gaps it identified between its current level of cyber maturity and the level required to achieve **SP–2 maturity across each of the 11 domains under the AESCSF framework**	Refer to section 2, specifically section 2.3 for discussion of the cost estimate. The initiative sequencing and estimated effort are discussed further in the ICT Cyber security baseline business case (8.72 RBC ICT Cyber Security Baseline – 31 Jan 23) submitted with the IRP.
Linking each of the above proposed actions to the respective individual costs required to undertake these actions	Refer to section 2, specifically section 2.3 for discussion of the cost estimate. We have expanded on this further in sections 2.4 and section 3, to demonstrate how we have developed the cost estimates for this program of works.
Detail for the individual costs inputs related to each proposed action, the basis for these costs (including relevant inputs, calculations, assumptions and sources) and set out how they were estimated, such as the number of labour-days or license fee	Refer to section 2, specifically section 2.3 for discussion of the cost estimate. We have expanded on this further in sections 2.4 and section 3, to demonstrate how we have developed the cost estimates for this program of works.
Demonstrating the efficiency of each cost input, e.g. through market testing and detailing all assumptions or other independent expert reports.	Refer to section 2, specifically section 2.3 for discussion of the cost estimate and steps we have undertaken to confirm the reasonableness of our cost estimate.

Contact

Australia: 1800 245 092
Overseas: +61 8 8923 4681
powerwater.com.au

PowerWater