

11 November 2022

Peter Gay
Head of Security Strategy
Transgrid
180 Thomas St
Sydney NSW 2000
Australia

Dear Peter

Re: Transgrid AER Pricing Review

Deloitte was asked to assist the Trustee for the NSW Electricity Networks Operations Trust (“Transgrid”) with an independent review of the cyber and physical security aspects of its 2023-28 revenue proposal in response to the Australian Energy Regulator (AER) draft decision to reduce Transgrid’s proposed 5-year Cyber Step Change OPEX from \$25M to \$13M. Deloitte was also asked to review the reasonableness of Transgrid’s cyber uplift initiatives against other market participants and, in the wider context, our understanding of cyber transformation programs.

The AER expressed concerns regarding the prudent and efficient application of proposed cyber expenditure by Transgrid. Prudent and efficient in the context of a cyber transformation program needs to consider the maturity trajectory of the organisation and whether they have taken a logical and methodical approach to address gaps and uplift capabilities. To be considered prudent, one needs to qualify the adequacy of the target state given the risk and legislative requirements that impact the entity, and to be efficient one needs to consider that the expenditure is reasonably justified and allows an agile responsiveness to risk, and a maturing cyber capability over time.

1. Scope

This letter provides an opinion in regard to the following aspects:

1. The cyber and physical security budget elements in the 2023-28 regulatory period to achieve and sustain SP-1, SP-2 and SP-3.
2. The cyber and physical security project timelines in the 2023-28 regulatory period to achieve and sustain SP-1, SP-2 and SP-3.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation” serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 312,000 people make an impact that matters at www.deloitte.com.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

3. Review of cyber and physical security scope in the 2018-23 regulatory period.
4. Potential factors and risks that may impact the accuracy of forecasting or insert additional cost/ time into the execution.
5. Cyber updates to be included in the December submission including any new activities and forecasts relating to legislative changes not well understood or final at the time of the initial submission – such as the Critical Infrastructure Risk Management Program.

2. Our Opinion – Management Summary

Deloitte reviewed the cyber and physical security aspects of Transgrid’s initial 2023-28 Revenue Proposal (dated January 2022) as well as the cyber and physical security aspects in the revised 2023-28 Revenue Proposal (to be submitted in December 2022). It is our opinion that Transgrid’s cyber and physical security funding submission is prudent to operate, maintain and mature Transgrid’s cyber capability, and is an efficient allocation of funding to operate baseline cyber capabilities, deliver on their strategic roadmap of initiatives, and meet regulatory obligations.

The following bullet points address each of the scope items:

- The proposed budget and timeline in the 2023-28 regulatory period to achieve and sustain SP-1, SP-2 and SP-3 is comparable with Australian energy industry norms, based on Deloitte’s experience of AESCSF cyber uplift programs in other market participants of similar size and position in the value chain. In addition, we would highlight the following:
 - Many areas of cyber and physical security uplift require an increase in recurring OPEX to sustain maturity. Actual, audited, FY2022 financial data has been used to calculate the base year OPEX required to sustain core cyber capabilities and maintain SP-1 in the 2023-28 regulatory period. Additionally, Transgrid requires an increased level of recurring OPEX to maintain SP-2 and SP-3. [REDACTED] To support this, Transgrid indicated they need to define a Common Operating Picture (COP) that will require significant resources and effort to capture the configuration of key platforms across the OT and IT environment, store them in a code repository, and monitor for deviations. As a result, the level of recurring-OPEX required to *maintain* an SP level once achieved is anticipated to rise.
 - [REDACTED] To address the evolving threat landscape, a proactive threat hunting and analysis service will require at least an additional \$750,000 per annum. This expense will continue through the current regulatory period and throughout the 2023-28 regulatory period as a recurring (base year) OPEX cost.
 - Few energy market participants have achieved SP-2 (or are even close to SP-2), so there is no robust data to compare the *actual* cost of SP-2 uplift versus the *planned* cost of SP-2 (and eventual SP-3) in peer organisations. This is made more complex by the limited number of Transmission Network Service Providers (TNSP) to benchmark against, and Transgrid being one of the largest. Only 21 (approximately 15%) of the 139 entities that have made submissions to the AEMO AESCSF Portal have achieved SP-1. Furthermore, only 1 of the 139 entities has achieved SP-2, with another 7 being close (approximately 5%). It is not understood which of these entities has had their maturity level validated independently, nor how many are TNSPs.

- Effort and funding required to reach SP-3 can only be based on modelling and comparing forecast expenditure as currently no energy market participants that have achieved SP-3 as yet (although a few are close) to obtain robust benchmarking data to validate the total costs, timelines, solutions, complexity, FTE uplift, and level of system and process integration required.
- Compliance with the AESCSF was previously assessed and planned by Transgrid based on Maturity Indicator Levels (MILs), which can be achieved for each of the 11 domains independently of each other. However, the shift to the concept of Security Profiles (SP) thresholds requires a more sequential approach because an organisation can only achieve a given SP if it achieves the required maturity level in every domain of the framework. While this may seem straightforward, it increases the complexity (time, cost and effort) required to progress from one SP to the next. For example SP-1 practices are mostly basic, relatively easy to achieve, and may be performed ad-hoc. Whereas the majority of SP-2 practices are more complex and advanced, requiring a methodical and enterprise-wide integrated approach. As a result of this added complexity, we believe it is reasonable for Transgrid to target SP-2 in the next regulatory period even though at a glance it appears they are very close to reaching that target [REDACTED]
- The basis for the proposed AER reduced budget (for the 2023-28 regulatory period) largely hinges on the expectation of Transgrid achieving SP-2 by June 2023, with the assumption this has been funded from the allowance within the 2018-23 regulatory period. However, it is unrealistic for Transgrid to achieve SP-2 by June 2023 based on a number of factors:
 - The AER and EMCa opinions are based on Transgrid's *self-assessed* maturity (completed in early 2021), which was used as an input to the original 2023-28 regulatory period submission. However, an independent review recently identified Transgrid's starting position was on average materially lower. This has increased the scope of work that needs to be undertaken to achieve SP-1, SP-2 and SP-3, as progress against individual domains within the AESCSF is in fact lower than originally understood.
 - [REDACTED] which resulted in resources being reprioritised to address the root cause(s), as would be reasonably expected from a prudent operator. Resultingly, this created additional priorities requiring management attention beyond those required as part of the AESCSF-aligned uplift, resulting in a natural slowing of progress.
 - Achieving SP-2 requires a considerable amount of uplift from the current position, which goes beyond just technology implementation. In common with other TNSPs and Distribution Network Service Providers (DNSPs), Transgrid has non-financial constraints as to how swiftly it can transform across 11 AESCSF domains in parallel, such as capacity for organisational change, regulatory conditions, and the bandwidth of (and access to) key staff and subject matter experts to support transformation workstreams.
- Transgrid's cyber and physical security activities and initiatives in the current regulatory period were prudent, and costs incurred for those activities and initiatives were reasonable:
 - The majority of cyber uplift work completed in the current regulatory period has focused on enhancing security, reducing risk, and executing programs of planned work, rather than solely considering AESCSF maturity as a focus of effort (noting that the AESCSF is itself one of many frameworks used to measure overall cyber maturity).
 - The increase in OPEX and CAPEX in the later years of the current regulatory period suggest Transgrid's willingness to invest in maturing their cyber capability. It is also reflective of the ongoing base year costs required to maintain cyber capability and SP-1 achievement.

- Transgrid's original submission for the 2023-28 period predated the assent of the SLACIP Bill (SOCl amendments), and the rules for industry are still being finalised. Consequently, it has been identified that first line and second line physical security assurance activities in the current regulatory period are not at the level required by the changes. The current base year OPEX for Physical Security [REDACTED] does not include an amount for the required uplift to first line or second line assurance activities. This needs to be funding through physical security Step Change OPEX. As a result, there should be no (\$0) base year adjustments for first line and second line physical security assurance activities.
- Transgrid's proposed 2023-28 regulatory period cyber budget (prepared in 2021 and revised in December 2022) is mostly focused on maturity uplift against AESCSF version 1. In our opinion, there are likely to be a range of factors that could drive additional funding requirements during the next regulatory period (2023-28). We recommend that these areas are also explored as part of the ongoing dialogue with the AER:
 - **A new version of AESCSF (v2) is imminent.** The Transgrid 2023-28 funding proposal is based on AESCSF version 1, which is itself based on a deprecated 2014 version of the US C2M2 standard (v1.1). AEMO and DISER have indicated that AESCSF version 2 is likely to be released in 'late 2022', which is likely to be aligned to C2M2 v2.1. Depending on the window for alignment, this change is likely to result in new requirements that will need to be planned and costed before 2028.
 - **The increased focus on risk management will result in a more granular understanding of vulnerabilities and risks to the transmission network.** The proposal predated the final version of the SLACIP amendments. This will require a Critical Infrastructure Risk Management Program to be developed. As part of that we expect that as Transgrid performs 'deep-dive' cyber risk assessments for critical assets that are essential to a safe and stable transmission network, this will uncover additional vulnerabilities or areas of concern, that are likely to result in (currently unquantified) funding requirements emerging to keep the risk within appetite.
 - **The cyber threat will continue to escalate.** The external cyber threat landscape is likely to continue escalating to 2028, which means cyber risk could still move outside of risk appetite despite a program of significant funding and uplift. In October 2022, ASIO highlighted cyber as being a preferred vector to target the energy sector for large scale destructive acts, with a goal of pre-positioning covert capability that may only become visible in a time-of-war. This is likely to lead to further efforts to discover vulnerabilities or weaknesses that could undermine the integrity of Transgrid's network.
 - **Cyber risk appetite is likely to shift in the event of a major cyber incident in transmission, or international conflict.** In our opinion, if there was a catastrophic cyber-related incident impacting another TNSP, or a major geo-political conflict in the Asia Pacific region, this is likely to result in a reduction in risk appetite around Transgrid's cyber posture. As such we anticipate any major cyber incident would be a driving force to accelerate initiatives or remediate risks that were previously deemed tolerable, thus ultimately increasing planned cyber spend.
- The Risk Management Program (RMP) rules in the SOCl Act require organisations to identify and mitigate material risks to critical infrastructure assets arising from: cyber and information security, personnel hazards, supply chain, and physical security and natural hazards. The RMP exposure draft is currently in consultation phase. Once that concludes, we expect market participants (including Transgrid) will have a short period of time to comply.
 - Deloitte reviewed Transgrid's additional RMP funding request which included \$9.5M to address overall RMP governance requirements, Supply Chain requirements, Personnel requirements and Physical Security for "Non-Network Sites". It is our opinion that this additional amount, and the related activities is on the lower side of what is necessary to provide a reasonable foundation for

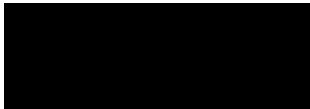
Transgrid to address the RMP rules in their current form. Furthermore, it is likely that the increasing complexity in this area will require specialist risk teams aligned with either the IT or OT environments. In our view Transgrid's RMP funding request is below the "RMP Regulation Impact Statement Costs" that the Department of Home Affairs submitted for the SLACIP Bill 2022 review in February 2022 (i.e. \$10.2M average one off cost and \$5.6M average annual ongoing cost for entities with critical electricity assets). It is likely that as the legislation evolves, stakeholder consultation is finalised, and the details are defined and clarified, that additional funding may need by Transgrid to align with the activities and expenditure required.

Note - Our review of Transgrid's RMP funding request was limited the "Attachment 7 - Protective Security and Resilience Business Case" document (dated 2 Nov 2022).

Our concluding opinion is that any reduction to Transgrid's Cyber OPEX funding will constrain it from adequately delivering a holistic program of cyber maturity uplift and risk reduction initiatives, and ongoing maintenance/operation of capabilities (both current and uplifted) necessary to achieve AESCSF SP-3. Moreover, the number of cyber developments since the original funding request and the likelihood of additional factors in the 2023-28 period (not least the volatility of cyber as a strategic threat) mean there is a high probability that additional cyber funding will be reasonably required within the 2023-28 regulatory period.

In drawing these conclusions we note that the Transgrid transmission network is rated as a "high" criticality market entity according to the AESCSF Electricity Criticality Assessment (E-CAT), due to the high potential of critical impact to wider Australian society (and other critical infrastructure entities) from a sustained core systems failure. This elevates the significance of the adequacy of cyber capability and risk management at Transgrid compared to other market participants.

Yours sincerely

A solid black rectangular box used to redact the signature of David Owen.

David Owen
Partner

Deloitte Risk Advisory Pty Ltd