TransGrid

TransGrid Revised Revenue Proposal
2018/19 – 2022/23

Appendix B

IT step change compliance with NSW license conditions

1. NSW licence condition compliance costs

TransGrid holds a licence issued under section 93A of the Electricity Supply Act 1995 (NSW) (Electricity Act) (Licence) by the NSW Minister for Energy (Minister) introduced on 7 December 2015. TransGrid must comply with the conditions of the Licence as well as various conditions from the Foreign Investment Review Board arising from TransGrid's change in ownership. There are 17 licence conditions of which three (6, 7 and 8) are referred to as the Critical Infrastructure Licence Conditions[1].

On an annual basis, in accordance with s88 of the Electricity Act, the Minister receives a report from the Independent Pricing and Regulatory Tribunal (IPART) as to the level of compliance by TransGrid against the Critical Infrastructure Licence Conditions (licence conditions). The licence conditions were drafted by agencies within the Federal Treasury and Federal Attorney Generals Department including the Foreign Investment Review Board (FIRB) and the Computer Emergency response Team (CERT).

The licence conditions acknowledge that the assets that TransGrid operates may constitute 'critical infrastructure' being those physical facilities, supply chains, information technologies and communication networks, which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the security, social or economic wellbeing of NSW and other states and territories[2].

Under the Licence, TransGrid must ensure that its transmission system can only be operated and controlled from within Australia (condition 6.1(b)). It must also ensure that it holds data on the quantum of electricity delivered and personal information, solely within Australia, and that this data is accessible only from within Australia (condition 7.1(a)).

TransGrid noted in its revenue proposal in January 2017, that IPART was yet to conclude its 2015/16 compliance report and TransGrid had not developed a compliant solution that met the NSW Government's licence conditions. After our revenue proposal was submitted, TransGrid's audit compliance report in relation to compliance with the licence conditions for IPART was finalised on 15 March 2017 and tabled in the NSW Parliament on 12 May 2017.

TransGrid's revenue proposal and subsequent documentation provided to the AER set out details for a step change covering additional costs associated with this regulatory change to be included in our maximum allowed revenue, for the 2018/19-2022/23 regulatory period, with a proposed amount of $14.4 million (2017/18). TransGrid developed a Program of Work in conjunction with the Federal Government agencies including CERT, the Critical Infrastructure Centre (CIC), FIRB and Federal Treasury ("Federal Agencies"). The Program of Work includes the implementation of technologies and processes to ensure compliance with the licence conditions and enhance the security of the critical infrastructure from, amongst other things, cyber attacks.

In 2017 TransGrid invested in a number of initiatives as a result of the licence conditions. The key compliance initiatives were implemented quickly to ensure compliance, [redacted]. The initiatives included:

[redacted]

1 Transmission Operator's Licence Under the Electricity Supply Act 1995 (NSW)
2 Transmission Operator's Licence Under the Electricity Supply Act 1995 (NSW), p.3.

- [redacted]

Several other initiatives have also been undertaken, including:

- completion of [redacted]
- completion of [redacted] assessment
- implementation [redacted]
- completion of [redacted]
- introduction of and improvement in capability of tools and instrumentation that provide ongoing monitoring and vetting of any [redacted]
- implementation of an ISO27001:2013 compliant Information Security Management System (ISMS) to define compliance policies and procedures taking into account TransGrid's regulatory obligations.

The AER, in its draft decision, agreed with TransGrid that a regulatory change has occurred in meeting the new licence conditions and included an alternative amount for the step change of $7.8 million (2017/18). The AER was not satisfied that TransGrid required the full cost increase[7]. The AER in making its draft decision considered IPART's 2015/16 audit report and supporting documentation and noted that TransGrid was due to submit a 2016/17 audit report to IPART and may consider taking this information into account as part of their final decision[8].

Since the AER's draft determination, in September 2017, the NSW government with input from the Federal Agencies and TransGrid has drafted revised licence conditions which are expected to be completed prior to the AER's final revenue determination in April 2018. The business needs and the amount of the allowance for the step change differs between the existing licence conditions and the final version of the revised licence conditions and the timing of any approval by the State and Commonwealth. Once signed by the NSW Minister, the amended licence conditions will take effect prospectively and not retrospectively. The Program of Work developed in conjunction with the Federal Agencies includes the transition plan containing the expected implementation steps required to be undertaken and forms part of amended licence conditions.

Therefore, TransGrid has prepared this step change submission, with its revised revenue submission, based on two possible outcomes:

- the step change allowance requirement under the retention of the "existing" licence conditions
- the step change allowance under the "proposed" licence conditions, if and when they become approved.

TransGrid is proceeding with this step change submission for covering incremental expenditure for the current conditions as well as the proposed conditions for the AER to consider prior to its final determination. The changes to the licence conditions include the introduction of documents to be approved by the Commonwealth and include a:

- protocol, for offshore remote access in exceptional circumstances, and

---

3 [redacted]

6 [redacted]

7 AER: Draft Decision: TransGrid transmission determination 2018 to 2023, p.7-47.

8 AER: Draft Decision TransGrid transmission determination 2018 to 2023, September 2017, p. 7-48

- transition plan, to provide a path to compliance by permitting TransGrid to undertake steps to enhance security.

The revised licence conditions will exempt TransGrid from the obligations under:

- both 6.1 and 6.2 when undertaking steps in accordance with the protocol
- 6.2 only when undertaking steps in accordance with the transition plan.

The following two sections summarise the alternate approaches required under the existing licence conditions and proposed licence conditions. A more detailed breakdown of the activities and costs are set out in section 4.6 and section 4.7.

1.1 Existing licence conditions

To meet the material change in TransGrid's regulatory obligations under the existing compliance requirements requires a revised incremental amount of $13.9 million to:

- continue on-shoring of [redacted], as per licence condition 6.1 (b)
- continue on-shoring of [redacted] as per licence conditions 7.1 (a)
- implementing technologies to achieve visibility and control of information flows [redacted] from overseas, as per licence conditions 6.1(b) and 7.1(a)
- recruiting a team of security and compliance specialists that maintain the additional compliance activities incurred by conditions 6 and 7, and ensure ongoing compliance; the ISMS policies and procedures will be operationalised and enforced by a compliance team to be established [redacted] and re-certified periodically. The team will also support compliance with the recently proposed Federal Draft Bill for Critical Infrastructure.

The required incremental step change under the existing licence conditions of $13.9 million is set out in the table below.

Table 1: TransGrid's existing licence conditions summary step change requirement, $ June 18

Compliance Category	2018/19	2019/20	2020/21	2021/22	2022/23	Total
SCADA onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Certification requirements	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Compliance staff - ISMS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**13,925,530**

1.2 Proposed licence conditions

Should the proposed licence conditions be approved, we will be able to reduce the costs of compliance with the licence conditions. To meet the proposed licence conditions requires:

- the implementation of a transition plan to be approved by the Commonwealth to ensure the steps undertaken as part of the plan will not cause non-compliance with 6.2; the transition plan will [redacted] and SCADA connections that are affecting TransGrid's business functions and increasing cost through incurred manual processes
- the implementation of technologies to achieve visibility and control of information flows to prevent remote access and data breaches, as per licence conditions 6.1(a) and (b) and 7.1(a), (b) and (c)
- building a team of security and compliance specialists that maintain the additional compliance activities incurred by conditions 6 and 7 and to ensure ongoing compliance

The compliance team will operationalise and enforce the ISMS policies and procedures in 2017/18 and support the annual re-certification process. This team will also support compliance with the recently proposed Federal Draft Bill for Critical Infrastructure.

TransGrid having completed the second audit and taking into consideration the proposed licence condition changes will require revised incremental compliance costs of $8.0 million over the upcoming regulatory period.

The required incremental step change under the proposed licence conditions of $8.0 million is set out in the table below.

Table 2: TransGrid's proposed licence conditions summary step change requirement, $ June 18

Compliance Category	2018/19	2019/20	2020/21	2021/22	2022/23	Total
SCADA onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Certification requirements	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Compliance staff - ISMS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**7,998,070**

1.3 Related Capital Expenditure Requirements

Whilst TransGrid has already invested in security related systems to meet the licence conditions there is a broader capital expenditure requirement to acquire and implement critical systems technology to enable the business and the security compliance team to manage its compliance regime against those licence conditions.

It is not possible to meet the licence conditions, existing and proposed, without these leading edge technologies in place. [redacted]

2. Summary of TransGrid's revenue proposal

TransGrid's revenue proposal set out details of an impending step change due to the introduction of the Transmission Operator's Licence conditions and various conditions from the Foreign Investment Review Board[9].

TransGrid noted in its revenue proposal, that IPART was yet to conclude its audit and TransGrid had [redacted] that met licence conditions and it was not possible at the time of the revenue submission to substantiate the expenditure requirements moving forward.

IPART published its 2015/16 audit report on 16 May 2017[10] and reported that TransGrid had not complied with two of the critical infrastructure conditions[11].

Subsequently, TransGrid submitted documentation to the AER supporting a step change request of $14.4 million over the upcoming regulatory control period, to meet the new compliance requirements. The documentation set out details of the relevant licence conditions, level of compliance achieved; what further actions were required, audit issues and the operating and capital expenditure requirement.

Documentation provided to the AER included:

- TransGrid-Brief to AER on new compliance requirements-0717, 5 July 2017- CONFIDENTIAL
- TransGrid-Finance and Support Services_IT Business case UPDATE-0717- CONFIDENTIAL
- TransGrid-IPART-Energy Networks Regulation Annual Report Revised-0517-CONFIDENTIAL
- response to AER questions including:
  - TransGrid-IR039-Step Change for New IT Compliance-20170725-CONFIDENTIAL
  - TransGrid-IR040-Opex Step Change-20170728-PUBLIC
- other supporting documentation, including copies of invoices showing the additional costs being incurred.

A summary of TransGrid's prior revenue proposal step change request is set out in the table below.

Table 3: TransGrid's revenue proposal step change requirement, $ June18

Compliance Category	2018/19	2019/20	2020/21	2021/22	2022/23	Total
SCADA onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Certification requirements	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Compliance staff - ISMS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] Licences	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**14,425,530**

[9] TransGrid: Revenue Proposal, 31 January 2017, p.153.

[10] IPART: Annual licence compliance report 2015-16, October 2016.

[11] IPART: Annual licence compliance report 2015-16, October 2016.

3. Summary of AER's Draft Decision

In the draft decision, the AER agrees with TransGrid that a regulatory change has occurred in meeting the new licence conditions and applied its standard approach to assess step changes[12]. However, the AER was not satisfied that the full step change increase for 2018/19-2022/23 (of $14.4 million) was required to comply with the licence conditions and included $7.8 million in its draft determination[13].

The AER in making its draft decision considered IPART's 2015/16 Audit report of TransGrid's compliance as well as supporting documentation.

In providing its draft determination the AER noted:

- that TransGrid was due to submit its 2016-17 audit report to IPART on 31 August
- IPART in turn must prepare a report to the Minister on the extent TransGrid has complied.

The AER may consider taking this information into account as part of their final decision[14].

4. TransGrid's updated step change proposal

4.1 Introduction

TransGrid is pleased that the AER recognises that a step change has occurred as a result of the regulatory change due to the introduction of new licencing conditions. Since submission of our revenue proposal to the AER there have been important updates including:

- release of IPART's 2016/17 audit report on TransGrid's compliance
- impending changes to the existing licence conditions, which are expected to be finalised prior to the AER's final determination in April 2018
- subject to Commonwealth approval:
  - the introduction of a protocol governing overseas remote access to TransGrid's systems in exceptional circumstances
  - inclusion of a transition plan to enable TransGrid to comply with its obligations regarding offshore access and control; whilst undertaking the necessary steps, as agreed with the Commonwealth, to enhance security of the network, with activities expected to commence in [redacted] and be completed by [redacted].

TransGrid confirms that all step change costs in this submission are incremental to any costs incurred in 2016/17.

4.2 Context of the challenges faced by TransGrid

Context for Federal Agencies licence condition requirements.

TransGrid recognises that the threats to its physical and virtual systems are genuine, global and increasing. This is demonstrated by a number of factors.

- Utilities were the target of 7.3% of global cyber incidents in 2016, up from 3% of total in 2014[15].

[12] AER: Draft Decision: TransGrid transmission determination 2018 to 2023, p.7-47.

[13] AER: Draft Decision TransGrid transmission determination 2018 to 2023, September 2017, p. 7-47.

[14] AER: Draft Decision TransGrid transmission determination 2018 to 2023, September 2017, p. 7-48

- In December 2015 an attack on a Ukrainian distribution utility cut power supply to 30 sub-stations and caused a six-hour power outage, impacting 225,000 customers[16]. The adversary also delayed restoration efforts by disabling control systems, disrupting communications and preventing automated system recovery. These effects were the result of over six months of planning and involved a range of activities, including compromise through spear phishing, the theft of user credentials through key loggers, and data exfiltration.[17] A subsequent attack on the Ukraine transmission network in December 2016 resulted in a significant outage to the capital city Kiev. This attack used automated malware tools to penetrate and compromise the internal network, and included advanced modules that were designed to automatically exploit transmission networks similar to TransGrid.
- A recent survey of US utilities ranked cyber security as 4.37 importance on a scale of 1 to 5 (where 5 is most important).
- The Cambridge Centre for Risk Studies estimates the potential losses for the United Kingdom resulting from a catastrophic attack on the power supply would be GBP442 billion over 5 years.
- An article in the Sydney Morning Herald, based on a recent survey from EY, challenged if Australia's power grid is safe from cyber threats[18].

Further, the increased digitisation of power networks and introduction of new, internet-enabled applications and distributed energy resources, is leading to a significantly more complex, connected landscape and the introduction of new threats that did not previously exist.

The threats also evolve and adapt to security measures constantly and quickly. TransGrid has progressively increased its investment in cyber security to secure its corporate data network in light of the increased global threat level and the increased risk posted to critical infrastructure[19]. This requires TransGrid to continually invest to maintain current levels of protection. Any degradation of TransGrid's capability relative to the threats will directly impact the resilience of critical infrastructure assets and systems.

As a result of these potential threats:

- power and water utilities globally have witnessed a surge in physical and cyber security spending since 2012 – up to 53% increase by some estimates[20]
- spending on cyber security is anticipated to increase at a compound annual growth rate (CAGR) of 9% to 2020 in utilities[21]
- 63% of utilities recently surveyed believe that digitisation has already resulted in increased cyber security investments and this trend is expected to continue to 2020[6]

We provide this context as these types of events and associated increasing risks of cyber activity, especially on electrical and data networks, are driving the federal and state governments to implement the strict licencing conditions on grid operators like TransGrid.

---

15 Symantec Internet Security Threat Reports, Black & Veatch: 2016 Strategic Directions: U.S. Electric Industry, Industry Research, Forbes

16 News Article, 2016, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", www.wired.com/2016/03/inside-cunning-unprecedented-hack- Ukraine's-power-grid

17 Australian Cyber Security Centre: *Threat Report* October 2016, pg. 18

18 The Sydney Morning Herald article "Cyber security threat: Is Australia's power grid safe from hackers?"; http://www.smh.com.au/business/energy/cyber-security-threat-is-australias-power-grid-safe-from-hackers-20171103-gze2qd.html

19 Australian Cyber Security Centre: *Threat Report* October 2016, pg. 17

20 PwC, 2017, "Global State of Information Security® Survey 2017"

21 IDC, 2016, "Global Cyber-Security Spending to Top $100B by 2020: IDC

4.3 Existing licence conditions and actions taken on the 2015/16 audit report

As stated previously TransGrid holds a Licence issued under section 93A of the Electricity Supply Act 1995 (NSW) (Electricity Act) (Licence) by the Minister for Energy (Minister).

The relevant sections are:

> Section 6: Substantial presence in Australia:
>
> 6.1 The Licence Holder must ensure:
>
> a. the maintenance of its transmission system is undertaken solely from within Australia, other than where such maintenance is not capable of being undertaken within Australia on reasonable commercial terms and conditions; and
>
> b. the operation and control of its transmission system is capable of being undertaken only from within Australia.
>
> Section 7: Data security
>
> 7.1 The Licence Holder must ensure that all:
>
> a. data as to the quantum of electricity delivered (both historical and current load demand) from or to any one or more sites (or their connection points);
>
> b. personal information within the meaning of the Privacy Act 1988 (Cth),
>
> relating to or obtained in connection with the operation of the transmission system by a Relevant Person is held solely within Australia, and is accessible only by a Relevant Person or a person who has been authorised by the Licence Holder and only from within Australia.

The 2015/16 audit report identifies two technical non-compliances in relation to two of the licence conditions, specifically licence conditions 6.1(b) and 7.1(a), where TransGrid was found to be in technical breach of the Licence for the period of 2015/16.

The actions that TransGrid immediately took in December 2016 when the audit report was delivered to mitigate those technical non-compliances [redacted].

To address the finding against section 6.1(b), [redacted] and on-shored the SCADA support services [redacted] and completely isolated the SCADA network. TransGrid's [redacted] SCADA systems from the planners, forecasters and engineers tasked with supporting the reliability of the transmission network and resulted in more manual effort and cost to achieve our regulatory and legal obligations to AEMO and the NEM.

To address data security requirements in section 7.1(a), TransGrid's IT service provider [redacted], is now delivering IT service operations from within Australia at additional cost.

TransGrid is working to find acceptable practical solutions to these restrictions. For example, as part of the new licence conditions a protocol has now been agreed which will allow remote access by [redacted] for emergency maintenance access. The protocol requires prior notification of relevant authorities and access to be observed by Federal cyber security experts from CERT Australia. It is intended that this protocol will be approved by the Commonwealth under the revised licence conditions such that TransGrid will not be in breach where it provides remote access in accordance with that protocol (refer above).

2016/17 Audit

On behalf of IPART, Hivint performed the 2016/17 annual audit of TransGrid's licence conditions during July to September 2017. This report was prepared for IPART and issued on 11 October 2017 and at the time of writing, the final ministerial acceptance of the audit report has not yet occurred.

The 2016/17 audit report found the same technical non-compliances for a portion of the 2016/17 audit period, from July to December 2016. This was due to the delay in the delivery of the previous 2015/16 audit, at which time TransGrid took immediate actions as set out above. TransGrid was otherwise compliant with the licence conditions.

A copy of Hivint's 2017 audit report prepared for IPART is at Attachment B1.

As discussed, to enable initial compliance with the licence conditions, TransGrid took a number of timely and temporary actions to physically separate access to systems by overseas service providers. More broadly, the actions included:

- delivering support onshore
- ensuring ongoing management and compliance capability is in place
- ensuring there is a level of operational capability to address potential cyber threats and other IT based disrupters
- implementing the ISMS and other initiatives.

To implement an ongoing compliance regime that has effective systems, processes and compliance capability requires an incremental step change, under the existing licence conditions of $13.9 million, as set out in the table below.

Table 4: TransGrid's step change requirement to meet existing licence conditions, $ June 18

Compliance Category	2018/19	2019/20	2020/21	2021/22	2022/23	Total
SCADA onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] onshore	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Certification requirements	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Compliance staff - ISMS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**13,925,530**

The activities being undertaken and a description of the costs are set out in Section 4.6.

4.4 Proposed licence conditions

The licence conditions are in the process of being amended and the proposed revised conditions were released by the NSW government in final form on 10 November 2017. The revised conditions include provision for the protocol and transition plan to be approved by the Commonwealth, exempting TransGrid from certain conditions when taking steps under those documents. The proposed amended licence conditions relevant for this step change are set out below:

"Section 6 Substantial presence in Australia:

6.1 Except to the extent allowed for under the *Protocol* agreed with the *Commonwealth Representative*, the *Licence Holder* must take all practical and reasonable steps to ensure:

a) the maintenance of its *transmission system* is undertaken solely from within Australia, except where maintenance requires either physical servicing of components offshore or the acquisition of replacement components from outside Australia. In such an instance it is the responsibility of the senior officer responsible for network operations to ensure this maintenance does not impact condition 6.2; and

6.2 Except to the extent that the Licence Holder is undertaking steps in accordance with, and for the duration of, a Transition Plan and/or a Protocol agreed with the Commonwealth Representative, the Licence Holder:

a) must, by using best industry practice for electricity network control systems, ensure that operation and control of its transmission system, including all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia, and that its transmission system is not connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside Australia;

b) must notify the Commonwealth Representative in advance of any engagement with the market to procure a contract under which it outsources the operation and control of its transmission system, including any ICT infrastructure associated with the operation and control of its transmission system.

Note: *For the purposes of Licence condition 6.2 (a);*

Best industry practice includes access required by relevant Australian regulators and market operators to meet the licence holder's obligations under Australian law.

Section 7 Data security

7.1 The Licence Holder must ensure that:

a) all of its information (being design specifications, operating manuals and the like) as to the operational technology (such as the SCADA system) and associated ICT infrastructure of the operational network is held solely within Australia, and that such information is accessible only by a Relevant Person who has been authorised by the Licence Holder and only from within Australia;

b) all:

(i) Load Data; and

(ii) Bulk Personal Data Records,

relating to or obtained in connection with the operation of the transmission system by a Relevant Person is held solely within Australia, and is accessible only by a Relevant Person or a person who has been authorised by the Licence Holder;

c) it does not export, and has appropriate security controls in place to prevent the export, of Bulk Personal Data Records relating to or obtained in connection with the operation of the transmission system by a Relevant Person, outside of Australia."

If the proposed licence condition changes proceed, the implementation of the remote maintenance access protocol in 2019/20 can replace the onshored SCADA support solution and provide a subsequent reduction in expenditure. [redacted] in

the transition plan will enable the offshoring of IT Services to be re-instated in [redacted]. Therefore, TransGrid has revised down our step change estimate to $8.0 million based on the proposed licence conditions.

The revised costs (dependent on the approval of the new licence conditions, protocol and transition plan) are set out in the table below.

Table 5: TransGrid's step change requirement to meet proposed licence conditions, $ June 18

Compliance Category	2018/19	2019/20	2020/21	2021/22	2022/23	Total
SCADA onshore/ remote access protocol support	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted] onshore	[redacted]	[redacted]				[redacted]
Certification requirements	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Compliance staff - ISMS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**7,998,070**

The activities being undertaken and a description if the costs are set out in Section 4.7.

4.5 Summary of TransGrid's Requirements to meet licence conditions

To meet the existing compliance requirements TransGrid is required to:

- maintain the onshore support activities from the system support service providers [redacted], as per licence conditions 6.1 (b) and 7.1(a)
- build a team of security and compliance specialists that maintain the additional compliance operating expenditure activities required by conditions 6 and 7, and ensure ongoing compliance. TransGrid has absorbed the capital expenditure cost in 2016/17 of implementing an ISO27001:2013 Information Security Management System (ISMS). The ISMS policies and procedures will be operationalised and enforced by this team in 2017/18 and re-certified periodically. The team will also support compliance with the recently proposed Federal Draft Bill for Critical Infrastructure
- implement the required technologies to achieve [redacted] as per licence conditions 6.1 (b) and 7.1(a).

If the proposed changes to the licence conditions are approved, it will allow TransGrid to reduce its requirements to:

- implement the steps set out in the Transition Plan (once finalised and approved). TransGrid has proposed a draft plan to the Commonwealth and state agencies, which is designed to achieve compliance with condition 6.2 and set out a Program of Work to strengthen security of the network whilst maintaining performance and reliability. This will securely restore the maintenance capabilities [redacted] removing the need for the current onshore arrangements by replacing the interim

arrangements and associated manual processes. The protocol which allows remote access will need management and monitoring processes to be implemented.

- build a smaller and less senior team of security and compliance specialists that maintain the additional compliance operating expenditure activities required by conditions 6 and 7, and ensure ongoing compliance. TransGrid has absorbed the capital expenditure cost in 2016/17 of implementing an ISO27001:2013 Information Security Management System (ISMS). The ISMS policies and procedures will be operationalised and enforced by this team in 2017/18 and re-certified periodically. The team will also support compliance with the recently proposed Federal Draft Bill for Critical Infrastructure
- implement the required technologies to achieve [redacted] as per licence conditions 6.1(a) and (b) and 7.1(a) (b) and (c).

4.6 Step change requirements under existing licence conditions

To meet compliance requirements under existing licence conditions TransGrid must implement a number of capital expenditure initiatives, and increase the operating expenditure required to implement the teams to operate sustainable security and compliance infrastructure and processes.

4.6.1 Expenditure to meet the existing Condition 6.1(b)

TransGrid's existing operating Licence includes "Condition 6.1(b): the holder of the Licence must ensure the operation and control of its transmission system is capable of being undertaken only from within Australia" which precludes the ability of any overseas entity from being able to access our control systems. It is critical to the stability and security of the transmission network that we are able to engage subject matter experts to assist in diagnosing and remediating any faults in the SCADA system.

For TransGrid to remain compliant with the licence conditions as interpreted by IPART, we are required to [redacted] for the next regulatory control period to provide an onshore technical resource to support the SCADA system.

4.6.2 Operating Expenditure to meet existing Condition 7.1(a)

TransGrid proposes to continue to use onshore IT services [redacted] to meet "licence condition 7.1(a): the holder of the Licence must ensure that Data as to the quantum of electricity delivered (both historical and current load demand) from or to any one or more sites (or their connection points) relating to or obtained in connection with the operation of the transmission system is held solely within Australia and is accessible only by an authorised person and only from within Australia." IPART had found in the 2016 audit that TransGrid was [redacted] IPART drew the conclusion [redacted]

To remain compliant with licence condition 7.1 (a) TransGrid required [redacted] to bring their IT services onshore at significant increased cost to TransGrid. The annual incremental cost is [redacted]. This results in an overall increased cost of [redacted] for the next regulatory control period.

4.6.3 Operating expenditure to meet existing Condition 7.1(a)

TransGrid's revenue proposal for the regulatory control period 2018/19-2022/23, included, [redacted] licence costs of [redacted]. The [redacted] Software as a Service offering was not continued to [redacted]. TransGrid

proposes to deliver a [redacted], on premise, thereby absorbing the related costs and not requiring a step change allowance for this.

4.6.4 Operating expenditure to meet existing Condition 7.1(a)

TransGrid has implemented the ISMS which define the policies and operational processes required to ensure information such as [redacted] within TransGrid is captured, stored securely, disseminated and destroyed in accordance with existing licence condition 7.1(a). To maintain compliance of ISO 27001:2013 for the ISMS an external annual re-certification is required. This external assurance would not be required without the additional compliance requirements imposed by the transmission operator's licence.

The ISMS also sets out the roles and responsibilities of the licensing compliance team. This operating expenditure represents the additional cost of annual surveillance audits and recertification audits every three years commencing in 2018/19. TransGrid requires an amount of [redacted] for the next regulatory control period for external annual re-certification of the ISMS. The cost estimate is based on [redacted] recertification during the next regulatory control period. A summary of these costs is set out in the table below.

Table 6: Annual recertification requirement costing, $ June18

Recertification Requirements	2018/19	2019/20	2020/21	2021/22	2022/23	Total
ISMS annual external reviews	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Enhancements to processes to maintain compliance (est.)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**488,330**

4.6.5 Operating expenditure to meet existing Condition 7.1(a)

TransGrid requires [redacted] to establish and maintain the security and compliance team in the upcoming regulatory period and service the maintenance and support costs associated with the required software.

The team will comprise a manager, [redacted] specialist IT security and compliance engineers and will provide 24/7 operation of the suite of processes and tools described below.

The team will perform the following operational tasks, supported by the procedures and policies of the ISMS.

1. Management, monitoring and maintenance of the [redacted] vulnerability management suite of tools used across IT and OT networks to maintain compliance of TransGrid's licence conditions 6.1(a) and 6.1(b) and requirements of Federal Agencies. These tools require updating and scheduling of scanning to check the current vulnerability state of systems. The output of these tools feeds into an operational process which requires [redacted] full time equivalent (FTE) effort by trained security staff to interpret the output and then advise TransGrid's service providers of required corrective action, perform assurance activities on progress and identifying areas of concern. Correct operation will enable TransGrid to minimise the threat of cyber attack through known

software vulnerabilities and meet the Australian Signals Directorate recommended "essential eight" cyber security controls.

2. Management, monitoring and maintenance of the logging of alerts and events from security incident and event management tools [redacted] correlate the output of vulnerability scans, or other unexpected activity that could cause an impact to the security and supply of the transmission network, and to maintain compliance with existing licence conditions 7.1(a). The effort to correlate, analyse and interpret this stream of information is estimated at [redacted] FTE.
3. Management, monitoring, maintenance and response to the alerts generated by the implementation of the [redacted] within the server and network environments. These tools identify and restrict movement of [redacted] and personal information and therefore permit TransGrid to remain fully compliant with existing licence conditions 7.1(a) and 7.1(b). The estimated effort to operate this toolset is [redacted] FTE.
4. Managing, monitoring and maintenance of the physical and logical separation technologies [redacted], policies and procedures that ensure load data remains accessible to Authorised Persons, to remain fully compliant with licence conditions 7.1(a). This separation of technologies will enable load data to be efficiently extracted from the SCADA systems. The estimated effort to operate this toolset is [redacted] FTE.
5. Management, monitoring and maintenance of [redacted] that use advanced techniques to detect and prevent insider threat activity that could impact the transmission network's stability and security, and alert on externally initiated cyber-attacks that could cause TransGrid to be not fully compliant with licence conditions 7.1(a) and 7.1(b). The estimated effort to operate this toolset is [redacted] FTE.

These projects described above at various stages of implementation with the intention of fully transitioning the operation of this suite of tools to the licensing compliance team in [redacted]. Currently the implementation project teams perform the operation of those tools that have been partially or fully implemented.

The table below sets out the details of the incremental costs associated with establishing a security and compliance team that are required for the next regulatory control period.

Table 7: Licensing compliance team costing, $ June18

Team	Position	Reports to:	Annual Salary	Total
Compliance Manager and three staff	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
Total			[redacted]	**1,121,400**

Note: Total includes annual salary, plus oncosts.

4.7 Step change requirements under proposed licence conditions

To meet compliance requirements under both existing and proposed licence conditions TransGrid must implement a number of capital expenditure initiatives, and increase the operating expenditure required to implement the teams to operate a sustainable security and compliance infrastructure and processes.

Details of these items are discussed further below.

4.7.1 Expenditure to meet the existing Condition 6.1(b) and proposed Conditions 6.1 and 6.2

TransGrid proposes to incur capital expenditure in the regulatory period to on-shore the support and maintenance functions performed by [redacted] on our SCADA system used to operate and control the transmission network, until such time as the remote maintenance access protocol is implemented in 2019.

TransGrid's existing Licence includes "Condition 6.1(b): the holder of the Licence must ensure the operation and control of its transmission system is capable of being undertaken only from within Australia" which precludes the ability of any overseas entity from being able to access our control systems. It is critical to the stability and security of the transmission network that we are able to engage subject matter experts to assist in diagnosing and remediating any faults in the SCADA system.

For TransGrid to remain compliant with the licence requirements as interpreted by IPART, we are required to pay [redacted]

The implementation of the remote access maintenance protocol and associated hardware and software would allow [redacted] with our licence conditions, approved by Federal Government. This will reduce incremental costs from [redacted] for the regulatory period, comprising [redacted] payments and then transitioning to internalised management and monitoring processes of the protocol arrangements.

4.7.2 Operating Expenditure to meet existing Condition 7.1(a) and proposed Conditions 7.1 (a) (b) (e) and (f)

TransGrid proposes to continue to use onshore IT services by [redacted] to meet "licence condition 7.1(a): the holder of the Licence must ensure that data as to the quantum of electricity delivered (both historical and current load demand) from or to any one or more sites (or their connection points) relating to or obtained in connection with the operation of the transmission system is held solely within Australia and is accessible only by an authorised person and only from within Australia." IPART had found in the 2016 audit that TransGrid was [redacted]

To remain compliant with licence condition 7.1 (a) TransGrid required [redacted] to bring their IT services onshore at significant increased cost to TransGrid. The annual incremental cost is [redacted] per annum, [redacted] when the completion of the [redacted] in conjunction with the ISMS secure storage procedures and compliance activities will ensure that offshore service providers [redacted].

This will reduce the total incremental costs from [redacted] to [redacted] for the next regulatory period.

4.7.3 Operating expenditure to meet existing Condition 7.1(a) and proposed Condition 7.1 (b)

TransGrid's revenue proposal for the regulatory period 2018/19-2022/23, included, [redacted] licence costs of [redacted]. The [redacted] Software as a Service proposal is withdrawn to remove any concerns around the [redacted]. TransGrid proposes to deliver a [redacted], on premise, thereby absorbing the related costs and not requiring a step change allowance for this.

4.7.4 Operating expenditure to meet existing Condition 7.1(a) and proposed Condition 7.1 (b)

TransGrid has implemented the ISMS which define the policies and operational processes required to ensure information within TransGrid is captured, stored securely, disseminated and destroyed in accordance with existing licence condition 7.1(a) and proposed Condition 7.1(b). To maintain compliance of ISO 27001:2013 for the ISMS an external annual re-certification is required. This external assurance would not be required without the additional compliance requirements imposed by the transmission operator's licence.

The ISMS also sets out the roles and responsibilities of the licensing compliance team. This operating expenditure represents the additional cost of annual surveillance audits and recertification audits every three years commencing in [redacted]. TransGrid requires an amount of [redacted] for the next regulatory period for external annual re-certification of the ISMS. The cost estimate is based [redacted] during the next regulatory control period. A summary of these costs is set out in the table below.

Table 8: Annual recertification requirement costing, $ June18

Recertification Requirements	2018/19	2019/20	2020/21	2021/22	2022/23	Total
ISMS annual external reviews	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Enhancements to processes to maintain compliance (est.)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	**488,330**

4.7.5 Operating expenditure to meet existing Condition 7.1(a) and proposed Condition 7.1 (a) and (b)

TransGrid requires a reduced incremental expenditure amount of [redacted] to establish and maintain the security and compliance team in the upcoming regulatory period and service the maintenance and support costs associated with the required software. TransGrid believes the proposed definition of Load Data in the draft licence condition 7.1(b) will require less maintenance effort from an operational perspective than the existing definition in the licence conditions.

The required amount has been reduced from TransGrid's proposed Step Change requirements as a result of the reduced compliance requirements in the draft licence condition changes.

The reduced team will comprise [redacted] IT security and compliance engineers and will provide 24/7 operation of the suite of processes and tools described below.

The team will perform the following operational tasks, supported by the procedures and policies of the ISMS.

1. Management, monitoring and maintenance of the [redacted] vulnerability management suite of tools used across IT and OT networks to maintain compliance of TransGrid's licence conditions 6.1(a) and 6.1(b) and requirements of Federal Agencies. These tools require updating and scheduling of scanning to check the current vulnerability state of systems. The output of these tools feeds into an operational process which requires [redacted] FTE effort by trained security staff to interpret the output and then advise TransGrid's service providers of required corrective action, perform assurance activities on progress and identifying areas of concern. Correct operation will enable TransGrid to minimise the threat of cyber attack through known software vulnerabilities and meet the Australian Signals Directorate recommended "essential eight" cyber security controls.
2. Management, monitoring and maintenance of the logging of alerts and events from security incident and event management tools [redacted], correlate the output of vulnerability scans, or other unexpected activity that could cause an impact to the security and supply of the transmission network, and to maintain compliance with existing licence conditions 7.1(a) and 7.1(b); The effort to correlate, analyse and interpret this stream of information is estimated at [redacted] FTE.
3. Management, monitoring, maintenance and response to the alerts generated by the implementation of the [redacted] within the server and network environments. These tools identify and restrict movement of [redacted] and personal information and therefore permit TransGrid to remain fully compliant with existing licence conditions 7.1(a) and 7.1(b). The estimated effort to operate this toolset is [redacted] FTE.
4. Managing, monitoring and maintenance of the physical and logical separation technologies [redacted]), policies and procedures that ensure load data remains accessible to Authorised Persons, to remain fully compliant with licence conditions 7.1(a). This separation of technologies will enable load data to be efficiently extracted from the SCADA systems and securely stored to remove the requirement for on-shoring of IT services. The estimated effort to operate this toolset is [redacted] FTE.
5. Management, monitoring and maintenance of [redacted] that use advanced techniques to detect and prevent insider threat activity that could impact the transmission network's stability and security, and alert on externally initiated cyber-attacks that could cause TransGrid to be not fully compliant with licence conditions 7.1(a) and 7.1(b). The estimated effort to operate this toolset is [redacted] FTE.

These projects described above at various stages of implementation with the intention of fully transitioning the operation of this suite of tools to the licensing compliance team in [redacted] Currently the implementation project teams perform the operation of those tools that have been partially or fully implemented.

The table below sets out the details of the incremental costs associated with establishing a security and compliance team that are required for the next regulatory period.

Table 9: Security and compliance team costing, $ June18

Team	Position	Reports to:	Annual Salary	Total
Compliance Team Leader and two staff	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
Total			[redacted]	**$774,300**

Note: Total includes annual salary plus oncosts.

5. Draft transition plan timeline

TransGrid has proposed to IPART, State and Federal representatives a transition plan under the proposed licence conditions designed to achieve compliance whilst ensuring the continued security and supply of the transmission network and information. The steps in the draft transition plan have been developed in consultation with Commonwealth representatives to ensure TransGrid can meet best industry practice in protecting the transmission from cyber-attack, as required under the amended conditions. The proposed transition plan will need to be approved by the Commonwealth and is therefore subject to change until the approval is obtained. Federal Treasury and Critical Infrastructure Centre have committed to participate with TransGrid and the AER in discussions as to direct relationships between the transition plan items and licence-related required compliance activities

5.1 Transition Plan

The program of work outlined in the transition plan is designed to replace ageing and no longer supported systems and will significantly add to the ability of the systems to withstand a cyber-attack. A draft transition plan and supporting details is being prepared in consultation with the Commonwealth, and once finalised, will be approved by the Commonwealth under the revised conditions. A high level timeline and activities is set out in the diagram below. The starting date will be set when approved, which is expected to be early December 2017.

A copy of the draft transition plan is at Attachment B2.

Table 1: Draft transition plan for revised licence conditions

Proposed Transition Plan