



Review of electricity network operators'
critical infrastructure licence conditions

Draft Report

November 2024

Energy >>

Acknowledgment of Country

IPART acknowledges the Traditional Custodians of the lands where we work and live. We pay respect to Elders both past and present.

We recognise the unique cultural and spiritual relationship and celebrate the contributions of First Nations peoples.

The Energy Networks Regulation Committee Members

The Energy Networks Regulation Committee members for this review are:

Jonathan Coppel, Chair

Peter Dunphy

Enquiries regarding this document should be directed to a staff member:

Jonathan Hopson

(02) 9019 1915

Matthew van Uffelen

(02) 9113 7789

Invitation for submissions

IPART invites comment on this document and encourages all interested parties to provide submissions addressing the matters discussed.

Submissions are due by Friday, 20 December 2024

We prefer to receive them electronically via our [online submission form](#).

You can also send comments by mail to:

Review of electricity network operators' critical infrastructure licence conditions

Independent Pricing and Regulatory Tribunal

PO Box K35

Haymarket Post Shop, Sydney NSW 1240

If you require assistance to make a submission (for example, if you would like to make a verbal submission) please contact one of the staff members listed above.

Late submissions may not be accepted at the discretion of the Tribunal. Our normal practice is to make submissions publicly available on our [website](#) as soon as possible after the closing date for submissions. If you wish to view copies of submissions but do not have access to the website, you can make alternative arrangements by telephoning one of the staff members listed above.

We may decide not to publish a submission, for example, if we consider it contains offensive or potentially defamatory information. We generally do not publish sensitive information. If your submission contains information that you do not wish to be publicly disclosed, please let us know when you make the submission. However, it could be disclosed under the *Government Information (Public Access) Act 2009* (NSW) or the *Independent Pricing and Regulatory Tribunal Act 1992* (NSW), or where otherwise required by law.

If you would like further information on making a submission, IPART's [submission policy](#) is available on our website.

The Independent Pricing and Regulatory Tribunal

IPART's independence is underpinned by an Act of Parliament. Further information on IPART can be obtained from [IPART's website](#).

Contents

1	We want to know what you think about network operators' critical infrastructure licence conditions	4
1.1	Executive Summary	4
1.2	Background	5
1.3	How this paper is structured	5
1.4	We encourage your input into the review	6
1.5	Review process and timing	6
2	Review context and approach	8
2.1	Review context	8
2.2	Review approach	10
2.3	We have improved the clarity of the conditions	15
3	Substantial presence in Australia	16
3.1	Maintenance of the transmission/distribution system	16
3.2	Access, operation and control of the transmission/distribution system	19
3.3	Australian citizenship and security clearance requirements	20
4	Data security	24
4.1	Holding information and data within Australia	24
4.2	Exceptions for complying with data security licence conditions	25
5	Compliance reporting and auditing	27
6	Full list of draft recommendations and questions	29
6.1	Recommendations	29
6.2	Questions	31

1 We want to know what you think about network operators' critical infrastructure licence conditions

1.1 Executive Summary

IPART has decided to conduct a review of the critical infrastructure licence conditions within the licences of Transgrid, Ausgrid, Endeavour Energy, Essential Energy and ACERZ (network operators). These conditions are contained within the licences in force under the *Electricity Supply Act 1995* (ES Act).

This draft report sets out our draft recommendations for critical infrastructure licence conditions. This draft report outlines the justifications and principles we considered in reviewing the licence conditions that we propose to recommend to the Minister.

The state's electricity supply is an essential service for consumers. The community and businesses rely on an electricity supply and they do not have an option to change to another network operator if they are dissatisfied with the level of security or reliability from that service. Regulation and licensing of network operators helps to achieve positive outcomes for the community and businesses in NSW by promoting the safe, efficient, and reliable operation of electricity networks.

We seek to ensure licence conditions are in the public interest and reflect public expectations, best practice and the licensees' circumstances. Licensing helps guard against adverse outcomes for an essential service. The current critical infrastructure licence conditions establish protections to support supply security and sovereignty, including cyber security.

The conditions require work to be conducted, information to be retained, and systems to be controlled from within Australia. They require a substantial presence within Australia, including that the boards contain Australian citizens and that key people within organisations pass security vetting. The critical infrastructure licence conditions support supply chain resilience, leading to greater reliability of the network. These conditions also help protect against foreign cyber threats that can threaten the security and reliability of the network.

Critical infrastructure licence conditions protect against significant risks. Left uncontrolled, these risks could manifest themselves with catastrophic consequences. This includes widespread severe customer impacts such as long-term shutdowns of services that result in significant losses to the NSW economy. Additionally, the reliability of supply is essential for people's way of life and particularly important for vulnerable and life support customers who are dependent on electricity.

It is against these imperatives that we have reviewed the current critical infrastructure licence conditions. We propose measured improvements that improve efficiency in monitoring compliance and network operators' ability to achieve security outcomes, recognise the current evolution of Commonwealth critical infrastructure frameworks, while also aiming to protect the people of NSW from risk.

1.2 Background

In 2022, IPART previously conducted a broader review of the licences where we considered it premature to make material recommendations on the critical infrastructure licence conditions at that time. Instead, we recommended that these conditions be reviewed after the national rules pertaining to the Risk Management Program under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) were embedded. This was because the changes under the Commonwealth framework may inform the recommendations to the licence conditions.

We are now conducting the review to assess whether the current critical infrastructure licence conditions are appropriate and for the following reasons:

- Amendments to the SOCI Act recently commenced,¹ which warrant the consideration of the amendment or removal of some of the critical infrastructure licence conditions.
- Conducting a review now is consistent with previous advice we provided to the then Minister for Energy in September 2022 (when we concluded our review of electricity network operators' licences). In November 2023, the Minister responded in support of the review.

This review is being conducted under IPART's regulatory functions under section 77(2)(b) of the ES Act in relation to the function of making recommendations to the Minister for or with respect to the imposition, variation or cancellation of conditions in relation to a licence.

1.3 How this paper is structured

The remainder of this Draft Report is divided into chapters that make it easy to identify the matters that are relevant to you. Chapters 3-6 contain an outline of the current critical infrastructure licence conditions along with our draft recommendations.

- **Chapter 2** discusses the context for our review and our approach, including what critical infrastructure is, what the obligations the current licence conditions contain, and the licensing principles design framework we will apply to the review.
- **Chapter 3** discusses our 'substantial presence in Australia' licence conditions, including obligations pertaining to:
 - maintaining, operating and controlling the transmission or distribution system within Australia
 - having directors who are Australian citizens and senior officers who hold security clearances and are responsible officers for operational technology, and network and security operations.
- **Chapter 4** discusses 'data security' licence conditions, including restrictions on holding, using and accessing data and information.
- **Chapter 5** discusses annual compliance reporting and auditing requirements.
- **Chapter 6** is a full list of the recommendations and questions contained in this draft report.

¹ These amendments included new obligations under the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (Cth).

1.4 We encourage your input into the review

We invite all interested stakeholders to make submissions in response to this Draft Report and the associated Draft Licence **by Friday 20 December 2024**.

We have listed specific recommendations as well as questions throughout this report where we invite your comment. You may also make a submission raising other issues that we have not covered in this paper in response to question 10.

You can provide input into our review by making a written submission to this Draft Report via our website.

We have provided a complete list of recommendations and questions at the end of this report in chapter 6. You do not have to respond to all recommendations and questions - you may choose to respond to only those that are important to you.

We look forward to receiving your submission. For more information on how to make a submission, our submissions policy, and how to manage confidential or commercially sensitive information in your submission, please see page ii at the front of this paper.

Have your say

Your input is critical to our review process.

[Submit feedback »](#)

You can get involved by making a submission in response to this draft report.

1.5 Review process and timing

This Draft Report sets out our preliminary views on the critical infrastructure licence obligations and poses questions where we seek stakeholder comment. We have also prepared a draft appendix that would replace the current critical infrastructure appendix in the licences. This draft appendix sets out our proposed critical infrastructure licence conditions.

We have provided an indicative timeline of our review below. The timing of the review will be subject to the number and complexity of submissions that we receive during consultation.

Once we have considered all stakeholder input on our draft package, we will finalise our recommendations, including the recommended licences and associated documents, and provide them to the Minister, who will make the final decisions.

We intend to provide our recommendation for amended licences to the Minister in early 2025. If we recommend changes to the current licence conditions, we intend to recommend that the Minister vary the licences so that the varied conditions become effective from 1 July 2025. The Minister will then consider whether to accept our recommendations.

Each final licence once granted by the Minister, would replace the current infrastructure appendix in the licence.



2 Review context and approach

2.1 Review context

2.1.1 What are the characteristics of the Network Operators and the differences between them?

The current licensed network operators are Transgrid, Ausgrid, Endeavour Energy, Essential Energy and ACEREZ².

Transgrid and ACEREZ are transmission network operators, whereas Ausgrid, Endeavour Energy and Essential Energy are distribution network operators. As transmission network operators, Transgrid and ACEREZ transmit electricity at high voltages, often between electricity generators and other electricity network operators in NSW and the ACT. Transgrid's network also connects to Victoria and Queensland. Transgrid has a small number of directly connected customers.

As distribution network operators, Ausgrid, Endeavour Energy and Essential Energy distribute electricity at lower voltages from the transmission network to end users including households and businesses.

2.1.2 What is critical infrastructure?

The preamble to the applicable network operators' critical infrastructure licence conditions provides that the assets the network operators operate 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 the State of New South Wales and other States and Territories which are from time to time electrically interconnected with New South Wales and other States and Territories.

2.1.3 What obligations are imposed by the current critical infrastructure licence conditions and what is the intent?

The current licences impose certain conditions on the electricity network businesses and protect the interests of the State and consumers. Current critical infrastructure licence conditions require the network operators to:

- have a substantial presence in Australia, including having:
 - maintenance, access, operation and control of the transmission or distribution system undertaken within Australia

² ACEREZ is a transmission network operator of the Central-West Orana Renewable Energy Zone and was granted a licence in September 2024.

- various citizenship, residency and security clearance requirements for directors and senior officers responsible for operational technology, and network and security operations
- have data security measures, including holding information within Australia, for operational technology information, load data, third party data and privacy of personal information
- comply with annual reporting and auditing requirements.

The risks to critical infrastructure are complex and have continued to evolve over recent years. Rapid technological change has resulted in critical infrastructure assets having increased cyber connectivity and greater participation in, and reliance on, global supply chains with many services being outsourced.

The intent of critical infrastructure licence conditions is to require that network operators protect their electricity networks from security threats by implementing physical, personnel and cyber security controls. These requirements help to ensure that licensed network operators can adequately manage business continuity, reliability, and network performance risks.

The critical infrastructure licence conditions are supported by audit guidelines and a reporting manual, which are issued by IPART and updated from time to time.

2.1.4 History of critical infrastructure licence conditions and overview of Essential Energy and ACERZ transition arrangements

Critical infrastructure licence conditions were included in Transgrid's licence in December 2015, Ausgrid's licence in December 2016 and Endeavour Energy's licence in June 2017 following the long-term lease of all or part of their assets by the then NSW Government.

Critical infrastructure licence conditions were included in Essential Energy's licence in February 2019. Until 30 June 2024, Essential Energy was following a *Critical Infrastructure Compliance Plan* (Approved Plan), which is a plan for Essential Energy to transition to compliance with its critical infrastructure licence conditions over a period of 5 years.³

Provided that Essential Energy took steps in accordance with the Approved Plan, Essential Energy was taken to have satisfied its critical infrastructure licence conditions for the duration of the Approved Plan.

We note the ACERZ licence, which was granted by the Minister in September 2024, currently contains transition requirements for the critical infrastructure conditions. The inclusion of these transitional requirements as part of our final licence recommendations are subject to the timing of the completion of this review and ACERZ's circumstances.

2.1.5 What is the regulatory framework?

IPART is responsible for monitoring and enforcing the network operators' compliance with critical infrastructure licence conditions.⁴

³ The term of the Approved Plan applied from 1 July 2019 to 30 June 2024.

⁴ Section 87(1) of the ES Act.

The Cyber and Infrastructure Security Centre (CISC) within the Commonwealth Department of Home Affairs also performs certain functions under the current critical infrastructure licence conditions.⁵ This includes approving Protocol agreements, assessing exemption applications from network operators for service providers to access data from overseas, and receiving annual compliance reporting.

IPART and the CISC work together closely to monitor the network operators' compliance with these licence conditions.

Additionally, licensed network operators have separate obligations under the SOCI Act since the electrical networks they operate are critical infrastructure assets. Critical electricity assets in the energy sector are of one of the 22 classes of assets across 11 sectors to which the SOCI Act applies. We have outlined the applicable SOCI obligations that relate to the licence conditions in the blue boxes throughout this report.

2.2 Review approach

2.2.1 We have applied our licensing principles to our review

We applied the following principles we developed when reviewing the critical infrastructure licence conditions.



Principle #1: Protect customers, consumers and the environment

We have designed licence conditions that drive beneficial outcomes for the people of NSW. The licence conditions:

- set necessary and appropriate regulatory requirements to achieve the desired outcome and address identified risks
- minimise social cost
- are in the public interest.



Principle #2: Proportionate and risk-based

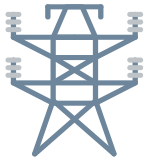
In designing licence conditions, we first identified risks for:

- electricity end users,
- the NSW electricity supply system,
- the community, and
- the environment

that the licence should address, and identified the outcomes we are seeking to address those risks.

We designed licence conditions that are effective in achieving these desired outcomes, proportionate to the licensed network operator's authority and influence to address those risks.

⁵ The CISC assists Australian critical infrastructure owners and operators to understand risk and meet regulatory requirements to collaboratively ensure the security, continuity and resilience of Australia's critical infrastructure.

**Principle #3: Facilitate efficient monitoring and enforcement of compliance**

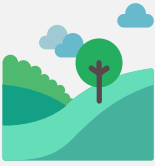
We designed licence conditions that facilitate IPART and co-regulators, such as the Cyber and Infrastructure Security Centre, to efficiently conduct their compliance monitoring and enforcement activities on licensed network operators. This includes clearly defined licence, audit and minimum reporting obligations necessary for us to be assured of the network operator's compliance with licence obligations.

**Principle #4: Avoid duplication where possible**

The licence conditions avoid duplication with other regulatory obligations to maximise efficiency, while recognising that it may be appropriate in some circumstances. For example, a duplicative condition may reflect government policy, legislation, an intergovernmental agreement or a court decision that requires inclusion of a licence condition.

**Principle #5: Facilitate efficient compliance with licence conditions by licensees**

We designed licence conditions that are outcomes focused and performance-based, not prescriptive. This allows licensees to find the most efficient way of delivering outcomes and encourages innovation. For example, we designed conditions that are technology neutral in achieving regulatory outcomes.



Principle #6: Promote safe, efficient, environmentally responsible and reliable electricity networks

We considered the statutory context of the ES Act when making recommendations about licence conditions. This includes:

- the objects of the ES Act:
 - to promote the efficient and environmentally responsible production and use of electricity and to deliver a safe and reliable supply of electricity, and
 - to confer on network operators such powers as are necessary to enable them to construct, operate, repair and maintain their electricity works, and
 - to promote and encourage the safety of persons and property in relation to the generation, transmission, distribution and use of electricity, and
 - to ensure that any significant disruption to the supply of electricity in an emergency is managed effectively.
- the statutory context of the licence being reviewed, including the subjects on which the Minister must grant conditions for.

2.2.2 Cost-benefit analysis

We do not propose to perform a detailed cost-benefit analysis on critical infrastructure licence conditions.

As outlined in section 2.1.2, the preamble to the critical infrastructure licence conditions, acknowledges that network operators have assets which, if destroyed, degraded or rendered unavailable for an extended period would have significant impacts (including economic) on NSW and other connected states or territories. The conditions are therefore intended to safeguard against threats and ensure the security of the network.

We therefore consider it is not preferable to do a cost-benefit analysis on the critical infrastructure licence conditions due to the low probability but potential for extremely high consequence of negative outcomes.

2.2.3 We have engaged an advisor to assist with our review

We have engaged CyberCX to assist with our review. CyberCX is an Australian consultancy with expertise in cyber security.

CyberCX has prepared a draft report containing recommendations against the current licence conditions which is included with this report.

We engaged CyberCX to review the licensed network operators⁶ current critical infrastructure licence conditions generally applicable to the licensed network operators for the purpose of informing our draft recommendations and draft licences. The main objective of the engagement was to advise on appropriate licence recommendations in the context of the:

- purpose of the critical infrastructure conditions in relation to the security risks of the electricity networks' operating environments,
- existing obligations and objectives of the SOCI Act.

We also required CyberCX to consider:

- overlaps or conflicting obligations between both regulatory regimes of the ES Act and the SOCI Act in order to reduce inefficiencies relating to operating under and complying with both regulatory regimes
- appropriate solutions that avoid duplication with the obligations of the SOCI Act and other relevant legislation, where it is possible
- opportunities to enhance the requirements under the current licence conditions or the principles and obligations under the SOCI Act where appropriate
- alternative licence conditions that are not inconsistent with the principles and objectives of the SOCI Act and the cyber security and critical infrastructure provisions of the ES Act.

CyberCX's recommendations have been based on CyberCX's key observation that the framework under the SOCI Act places principles-based obligations on network operators to manage 'material risks' via a risk management program. This is in contrast to the licence conditions which CyberCX and the CISC consider sets a higher security standard.

CyberCX has made risk-based recommendations with the primary aim of ensuring the conditions support the network operators to preserve the security and availability of NSW's electricity supply. In the process, CyberCX considered the potential for network threats and vulnerabilities arising from its recommendations given its expertise in cyber security. CyberCX also took into account our licensing principles.

We have considered CyberCX's recommendations in forming our draft recommendations to the Minister.

We have generally adopted CyberCX's recommendations. We have outlined CyberCX's recommendations in Chapters 3 to 5 of this report and also indicated where we propose not to adopt its recommendations.

⁶ For the purposes of this review, CyberCX considered the critical infrastructure licence conditions as a single and equivalent set which are applicable across the licence holders at the time of the engagement (i.e CyberCX's advice did not distinguish between the licensed network operators). The ACEREZ licence was granted during the engagement.

2.2.4 We have considered requirements of the ES Act when reviewing the licence conditions

Clause 6(5) of Schedule 2 to the ES Act requires the Minister to impose certain conditions on each licence. Relevantly, clause 6(5)(c) states:

6 Conditions of licences

(5) Without limitation, the Minister must impose the following conditions on each licence—

....

(c) conditions for ensuring that a network operator maintains a substantial operational presence in Australia.

The current licence conditions contain obligations to meet these requirements. In addition, a licence is subject to such other conditions (not inconsistent with the ES Act and regulations) as the Minister may impose from time to time.

We have considered this 'substantial presence' requirement when reviewing the critical infrastructure licence conditions to ensure that our recommendations to the Minister for any new or amended licence conditions satisfy this requirement.⁷

2.2.5 We have considered reporting manuals and audit guidelines

The Network Operators' licences include conditions requiring them to provide reports to IPART on their compliance with particular obligations. IPART issues reporting manuals that further specify these reporting requirements, and include information such as report contents, due dates and report recipients. The *Electricity networks reporting manual – Critical infrastructure licence conditions* (Reporting Manual – Critical Infrastructure) specifies reporting requirements for critical infrastructure licence conditions.

The current Network Operators' licences require them to comply with any reporting manuals issued by IPART. This means that a non-compliance with an obligation in the reporting manual is a non-compliance with a licence condition.

The *Electricity networks audit guideline – Audit fundamentals, process and findings* (Audit Guideline – Audit Fundamentals) sets our expectations regarding the conduct of audits of electricity networks' licence and safety obligations. The *Electricity networks audit guideline – Critical infrastructure licence conditions audits* (Audit Guideline – Critical Infrastructure) sets our expectations regarding the conduct of audits of critical infrastructure licence conditions.

We have reviewed the above reporting manual and the audit guidelines and found no pressing need to amend and consult on these documents as part of this review. We will review these documents at a later date to ensure the requirements under these documents are consistent with any associated licence conditions prior to the licence conditions taking effect. However, if stakeholders raise issues relating to these documents, we will consider these issues and address them if required.

⁷ Please refer to section 2.1.3 for an overview of the current obligations under the 'Substantial presence in Australia' requirement.

Seek Comment



1. Do you consider the critical infrastructure reporting manual and applicable audit guidelines contain significant issues in complying the requirements of these documents, and if so, what are these issues?

2.3 We have improved the clarity of the conditions

We consider the existing critical infrastructure licence conditions within the Transgrid, Ausgrid, Endeavour Energy and Essential Energy licences could be more clearly articulated. We have made plain English and structural changes to these draft conditions to improve the readability and assist network operator's interpretation of the licence conditions. We expect this will facilitate regulators (including IPART) to efficiently monitor for compliance.

Note as we have applied the structural and readability changes throughout the draft licence, we have not referred to each of the individual wording changes specifically in each of the recommendations of this report for brevity. For example, a recommendation to amend a licence condition is only in relation to an amendment to the requirement or the principle of the condition, and not the wording.

3 Substantial presence in Australia

The ES Act requires that the Minister impose on each licence "conditions for ensuring that a network operator maintains a substantial operational presence in Australia".⁸

The current licence conditions require work to be conducted, information to be retained, and control to be accessible from within Australia. The current conditions also require that boards or governing bodies contain Australian citizens and that key people within organisations pass security checks.

We consider the critical infrastructure licence conditions should support supply security and sovereignty, including security against malicious control of the network. We consider such conditions would also be expected to support supply chain resilience, leading to greater reliability of, and security of supply for, the network.

These conditions also help protect against foreign threats, which may be beyond Australian laws and powers, that could threaten the reliability of the network.

We have made recommendations in the sections below to ensure network operators continue to have a substantial presence in Australia and implement appropriate controls to ensure the security of their networks.

These protections and requirements are important since electricity networks are an essential service for the people of NSW.

3.1 Maintenance of the transmission/distribution system

Draft recommendation

1. That the critical infrastructure licence conditions:
 - Retain the requirement that the licence holder must take all practical and reasonable steps to ensure that maintenance of the transmission or distribution system is undertaken solely from within Australia.
 - Amend the current requirement for the senior officer responsible approve any third party maintenance of the distribution system to instead permit the network operators to acquire, or conduct physical servicing of components from outside Australia, for the purposes of maintenance of the distribution or transmission system where:
 - it is not reasonably practicable to acquire the components or conduct physical servicing from within Australia, and

⁸ ES Act, Sch 2 clause 6(5)(c).

- the Senior Officer Responsible for Network Operations approves acquisition from, or physical servicing by, a specific person or entity from outside of Australia.
- Retain the current exceptions to the above requirement where a protocol is established with the Commonwealth regulator.

Our draft recommendation is to generally retain the current obligations. These obligations ensure that the network operators have controls in place to manage the risk of maintenance activities (such as offshore component servicing and acquisition) being carried out by external parties.

While the SOCI Act⁹ has relevant requirements (see box below) we consider that the licence condition is a more stringent obligation with more specific requirements. That is, the requirements under the SOCI Act achieve a lower standard of security than the licence requirement and therefore removing the licence requirements could result in greater risk exposure. We consider a higher security standard to be necessary and as a result we do not consider this recommendation to be a duplicate of the requirements under the SOCI Act.

We note the current licences contain a requirement that *any* third party or non-licence holder employee, including individuals/entities from outside Australia, undertaking maintenance of the transmission or distribution system is subject to the approval of the senior officer responsible for network operations. We consider this licence condition may be unnecessarily broad and may cause interpretation issues implying that all third party maintenance activities should be subject to senior officer approval even including from domestic third party contractors. This could lead to unintended outcomes such as process delays to necessary network repairs.

As a result, we propose to clarify this condition. We have amended the draft condition to permit that acquisition or physical servicing of components, from a specific person or entity outside Australia, for the purpose of maintenance of the system. This is only permitted insofar as it is not reasonably practicable to acquire the components, or conduct physical servicing, from within Australia, and if the senior officer responsible for network operations has approved the acquisition or physical servicing by a specific person or entity.

CyberCX recommended the licence include a condition to enable virtual servicing from external third parties including from overseas providers. CyberCX considered this could be achieved by establishing a 'test environment' that would be physically separated from the operational environment.

We do not propose to adopt CyberCX's recommendation to allow for virtual servicing. We consider this would create the potential for an unacceptable level of risk exposure to the security of the networks due to increased likelihood of external attacks arising from increased access.

The CISC agrees with this position and also considers the use of virtual servicing to be high risk. This is because once data is transferred to an external service provider, including from outside of Australia, there is a loss of visibility and control with this data, even with controls in place.

⁹ Including related requirements such as the Risk Management Program Rules.

Additionally, we consider such a requirement would likely introduce significant complexities that would impact our compliance monitoring role and also a network operator's ability to comply with its licence obligations. This is because the licence would need to contain sufficient specificity and definitions for key concepts, the minimum level of controls and the types of activities permitted or not permitted. Ultimately, any new requirement should not significantly impact a network operator's ability to maintain operation and control of the network and prevent the access of sensitive information from outside Australia.

We acknowledge the substantial presence requirements may impose restrictions on local activity and access to expertise and so we propose to maintain the current exemption requirements. As a result, network operators may enter into a Protocol agreed with the CISC for alternative maintenance arrangements. The CISC supports this arrangement.

While we expect most of the physical work on the network requires people to work on it domestically, we also understand that there may not be local suppliers of certain components. Allowing for the limitations of the domestic market helps to minimise the social cost of this condition.


The exemption to establish a protocol with the CISC enables the network operator to put in place alternate controls which achieve an acceptable level of risk at a lower cost, thereby facilitating efficient compliance with the licence conditions by licensees.

Relevant SOCI obligations – maintenance of the distribution or transmission system

SOCI entities must have, and comply with, a critical infrastructure risk management program to address the following requirements:

- as far as it is reasonably practicable to do so, minimise or eliminate the material risk associated with remote access to operational control or operational monitoring systems of the asset.
- permit a critical worker access to critical components of the critical infrastructure asset only where the critical worker has been assessed to be suitable to have such access

Seek Comment

-  2. Do you agree with our proposal to retain the maintenance of the distribution/transmission system conditions?
3. Do you agree with our proposal to retain the exception to the maintenance condition allowing for a protocol to be agreed with the CISC?

3.2 Access, operation and control of the transmission/distribution system

Draft recommendation

2. That the critical infrastructure licence conditions:
- Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that the system, and all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia.
 - Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that the requirement that the system is not connected to any infrastructure or network in a way that could enable a person outside Australia to access, control or operate it in whole or in part.
 - Retain the requirement that the licence holder notify the Commonwealth Representative in advance of any engagement with the market to outsource operation and control of the system.
 - Retain the exception to the above requirements where a protocol is established with the Commonwealth regulator.

The conditions protect against access, control and operation of the network from outside of Australia. The condition provides a 'best industry practice' test so that controls are reasonable and remain contemporary as technology changes. To allow flexibility, an exception to this condition may be established through the establishment with a protocol with the Commonwealth regulator.

These obligations ensure that:

- the network operators have appropriate controls in place to prevent the transmission/distribution system from being accessed, operated or controlled from outside of Australia and therefore they help to support the security and availability of the network.
- the Commonwealth Representative is able to assess the security risk of a network operator potentially outsourcing the operation and control of its transmission/distribution system.

i Relevant SOCI obligations – operation and control

SOCI entities must have, and comply with, a critical infrastructure risk management program (CIRMP) to address the following requirement:

- as far as it is reasonably practicable to do so, minimise or eliminate the material risk associated with an interference with the asset's operational technology or information communication technology essential to the functioning of the asset.

3.2.1 We propose to maintain the requirements for the access, operation and control of the transmission/distribution system

Our draft recommendation is to retain the current obligation that, except where allowed for under a protocol, a network operator must ensure the operation and control of transmission/distribution system from within Australia.

We agree with CyberCX's view to maintain the requirements. We do not consider it appropriate to defer to the SOCI Act at this time as the licence condition includes more specific requirements than the SOCI Act, and given the high consequence of unauthorised access and control of a network.

CyberCX's report cites previous international cases where a foreign entity gained unauthorised access to an electricity system. Such access has the potential for extremely high consequences as a malicious attack on a network could cause damage to the electricity infrastructure and/or disable the power supply for a period of time. System outages would have large repercussions on the security, social and economic wellbeing of citizens.

We do not propose to further specify the term "best industry practice" relating to managing control of a transmission/distribution network as the network operators currently achieve this licence requirement using a variety of different controls, standards and frameworks. This proposed approach is also in line with our licensing principle of allowing licensees to find the most efficient way of delivering outcomes that are technology neutral in achieving regulatory outcomes.

We therefore conder retaining this requirement to be important for supporting supply security and sovereignty, including security over the malicious activities from external and unauthorized control of the network.

Seek Comment



4. Do you agree with our proposal to maintain the requirements for operation and control of the transmission/distribution system?

3.3 Australian citizenship and security clearance requirements

Draft recommendation



3. That the critical infrastructure licence conditions:
- Maintain the requirement for at least two directors to be Australian citizens.
 - Amend the security clearance requirements, so that at least two directors and any senior officers responsible for operational technology, network operations and security operations must either undertake an AusCheck background check or hold a Negative Vetting Level 1 clearance. Where an AusCheck background check is used, the network operator will be required to reasonably ensure the person does not present a security risk.

- Maintain the exemptions and obligations relating to the timeframes for appointing directors and senior officers responsible in the event of a vacancy subject to amendments to:
 - reduce the maximum allowable timeframe from 8 months to 4 months to achieve compliance with obtaining a national security clearance or have undertaken a Background Check following a vacancy
 - include an additional condition enabling the licence holder to nominate a longer exemption period for IPART's approval.

The ES Act requires that the Minister must impose licence "conditions for ensuring that a network operator maintains a substantial operational presence in Australia". We consider these requirements for a substantial Australian presence apply to network operator personnel, and that the licence should contain requirements around a network operator's senior personnel and members of the governing bodies who could have significant influence on the nature of the operations.

The current conditions require licence holders to have at least two directors who hold Australian citizenship and any senior officers responsible for operational technology, network operations and security operations, to reside in Australia. Additionally, the current conditions require certain officers hold a national security clearance, being a clearance of not less than Negative Vetting Level 1 (or equivalent) issued by the NSW Government on advice from the Australian Government Security Vetting Agency (AGSVA).

We note AGSVA's security clearances require an appropriate sponsoring agency as part of the application process as individuals cannot sponsor their own security clearance. We have therefore maintained the wording requiring the NSW Government's involvement.

Relevant SOCI obligations – Australian citizenship and security clearance requirements

The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (Cth) Risk Management Program Rules require network operators to identify critical workers and eliminate or minimise material risks associated with critical workers and mitigate, so far as is reasonably practicable, the relevant impact of such hazards (e.g arising from malicious or negligent employees or contractors). The Risk Management Program Rules specify the AusCheck scheme (which conducts background checks) as a possible method for assessing the suitability of a critical worker. If the AusCheck scheme is used, the background check must include information regarding specific matters, including a security assessment.

3.3.1 We propose to maintain a citizenship requirement

We consider that a citizenship requirement helps to support a substantial presence in Australia. This condition helps to ensure a degree of strategic influence from Australians who have a connection with the community they are serving and are subject to Australian jurisdiction.

We expect other frameworks may also have citizenship requirements and that this reduces the burden of this condition. Essential Energy is a state-owned corporation under the *State Owned Corporations Act 1989* where board members are appointed by the Governor on the recommendation of the voting shareholders. Certain other network operators are subject to Foreign Investment Review Board requirements which also include a requirement that a specified number of board members are citizens.

3.3.2 We propose to amend the security clearance requirements for senior officers and directors

We consider the licence conditions should specify a minimum level of security requirements for its key personnel relating to its senior officers and directors. We consider the integrity and resistance to extortion of these key positions to be important in protecting against influence from bad actors. This is also in line with other critical infrastructure sectors such as aviation and maritime.

We agree with CyberCX's recommendations to amend the security clearance requirements relating to the senior officers and directors.

CyberCX considers the use of AusCheck background checks is a sufficient means to meet the personnel security requirements, and an acceptable alternative for the current NV1 security clearance requirements.

Although CyberCX recommended the AusCheck background checks could replace the NV1 security clearance requirements, we propose instead to amend the security requirements to provide additional flexibility. We propose to allow directors and senior officers responsible to undertake an AusCheck background check or NV1 security clearance. We have specified that a network operators may continue to achieve the security requirements by obtaining NV1 security clearance as it is a more comprehensive security assessment compared to AusCheck.

We consider allowing a network operator to have the flexibility to choose between undertaking an AusCheck background check or NV1 security clearance is appropriate. This proposed recommendation recognises that some existing network operator key personnel already hold NV1 security clearances or that a network operator's preferred practice may be to obtain a higher level security clearance with the NV1 over an AusCheck background check.

Where an AusCheck is being used, we propose that the licence holder is to reasonably ensure that the person subject to the AusCheck is not a security risk. This is because AusCheck findings return either a 'clear' or 'adverse findings'. As a result, an AusCheck produces, among other things, a national security assessment which an entity must take into account in determining whether it is suitable for a person to have access to sensitive information or critical assets.

We understand the AGSVA security clearances may be subject to extended processing times. Additional process delays could also impact the network operators' ability to meet the intent of the licence conditions to ensure that its senior personnel responsible for managing the security of the network have adequate clearances in place. This supports our recommendation to amend the requirements relating to NV1 to also allow for an AusCheck.

Further, the CISC has supported the recommendation to allow an AusCheck background check as an alternative for obtaining the background checks as it is more accessible to industry and is generally a quicker process compared to NV1, noting that it is not as robust.

We consider our proposed amendment to also allow for an AusCheck background check, this reduces the regulatory burden and is consistent with our licensing principles to protect consumers while also being proportionate. This is because the security requirements for an AusCheck background check help protect against bad actors occupying critical positions while being less stringent and less resource intensive than those required by a NV1 security clearance.

3.3.3 We propose to largely maintain requirements on appointing directors and senior officers in the event of a vacancy

The current conditions impose constraints around the exemptions relating to the timeframes for appointing directors and senior officers and their applications for national security clearance in the event of a vacancy.

We propose to maintain the substance of these requirements but also simplify the requirements to improve interpretation and compliance monitoring. With the proposed introduction of an AusCheck background check in the licence as an alternative to holding NV1 security clearance, we consider the current 8-month allowance can be reduced and simplified to 4 months. However, we also acknowledge that the timeframes for obtaining clearances or checks are subject to processing times outside the direct control of the network operator and as a result the draft licence includes an additional condition enabling the licence holders to nominate a longer period for IPART's approval.

Seek Comment



5. Do you agree with our proposal to amend the security clearance requirements by allowing a network operator to choose between NV1 security clearance or the background checks under the AusCheck scheme?

4 Data security

4.1 Holding information and data within Australia

Recommendations

4. That the critical infrastructure licence conditions:
- Maintain the requirement that all Operational Technology Information is held solely in Australia only accessible from within Australia by a Relevant Person who has been authorised by the Licence Holder.
 - Maintain the requirement that Load Data relating to, or obtained in connection with, the operation of the Distribution or Transmission System by a Relevant Person is held solely within Australia, and only accessible from within Australia by a person who has been authorised by the Licence Holder.
 - Maintain the requirement that Third Party Data indirectly accessed or obtained because a Carrier or another person transferred the Third Party Data using the Licence Holder's infrastructure is held solely within Australia, and only accessible from within Australia by a person who has been authorised by the Licence Holder.
 - Remove the requirement that Bulk Personal Data Records are subject to conditions within the licence.

We consider that the security of Operational Technology information is of critical importance to protecting the Transmission/Distribution system against malicious attacks by bad actors. We expect this information may reveal system vulnerabilities which could be exploited to gain access or control of the system.

Retaining Operational Technology information within Australia enables greater control over it and protection of it. We consider it likely that security arrangements within Australia may be better managed. In addition, surveillance and enforcement activities by Australian security agencies are more likely to be effective from within Australia.

We note in the draft licence conditions, we propose to consolidate a number of the existing data security licence conditions requiring certain information be held and accessed within Australia. As a result, the draft licence refers to operational technology, load data and third party data under the single term 'sensitive information' whereby such information is required to be held and accessed in Australia.

Relevant SOCI obligations – Data security

SOCI entities must have, and comply with, a critical infrastructure risk management program (CIRMP) to address the following requirements:

Relevant SOCI obligations – Data security

- as far as it is reasonably practicable to do so, minimise or eliminate the material risk associated with storage, transmission or processing of sensitive operational information outside Australia
- as far as it is reasonably practicable to do so, minimise or eliminate the material risk associated with remote access to operational control or operational monitoring systems of the critical infrastructure asset.

4.1.1 We propose to remove the requirements for Bulk Personal Data Records

The *Privacy Act 1988* (Cth) (Privacy Act) regulates the way personal information is handled. It applies to agencies, and organisations with an annual turnover of \$3 million or more, subject to some exceptions. The Privacy Act sets out 13 Australian Privacy Principles that govern standards, rights and obligations of the collection, use and disclosure of personal information. The licensed network operators must not do anything, or engage in a practice, that breaches any of these principles.¹⁰ The Privacy Act also provides penalties for serious or repeated breaches of any of these principles.

We consider that requirements related to Bulk Personal Data Records are no longer required by the licence. We agree with CyberCX that the requirements set out in the Privacy Act, particularly the Australian Privacy Principles 8 (cross-border disclosure of personal information) and 11 (security of personal information) perform the same role as the licence conditions. We therefore consider the licence requirements around Bulk Personal Data Records to be duplicative and unnecessary.

Seek Comment



6. Do you agree with our proposal to retain the data security requirements?
7. Do you agree with our proposal to remove the Bulk Personal Data requirements?

4.2 Exceptions for complying with data security licence conditions

Recommendations



5. That the critical infrastructure licence conditions:
 - Maintain the exemptions to the Data Security requirements,

¹⁰ Section 15 of the Privacy Act.

- Replace the provisions, allowing the Commonwealth Representative or IPART to agree in writing to other arrangements, with a provision enabling the Commonwealth Representative to agree to a Protocol as an alternate to comply with the data security licence conditions.
- Maintain that existing approvals and arrangements granted or agreed to by IPART or the Commonwealth Representative under the current licences remain in force.

We propose to substantially maintain the current licence conditions around the exemptions to comply with the data security requirements.

We consider these exemptions are necessary as they support circumstances where from time to time a network operator or a third party is required to disclose, hold, use or access any of the information referred to in the previous section for legitimate reasons such as legal, regulatory, industry, financial reasons or other reasons. The absence of such exemptions may present an impracticable barrier to the effective operation of the network and its required business practices.

We propose to replace two of the current exemptions with an expanded Protocol referenced in the substantial presence in Australia conditions discussed in section 3 of this report. The two exemptions relate to approvals given by IPART or arrangements agreed to by the CISC. For consistency and clarity, we propose to replace these provisions with a single Protocol (any pre-existing arrangements will continue to be valid and do not have to be incorporated into the protocol).

This Protocol may also cover items in other parts of the licence. A Protocol with the CISC involves a formal risk assessment process requiring the network operator to provide details on the nature of the exception being sought and demonstrate that appropriate controls would be in place to ensure information security.

The CISC supports this recommendation to broaden the use of a Protocol for use on a case-by-case basis as it allows a formal mechanism for the CISC to assess the residual offshore data security risk.

Seek Comment



8. Do you agree with our proposal to replace the data agreement provisions with a new provision enabling the Commonwealth Representative to agree to a Protocol?

5 Compliance reporting and auditing

6. That the critical infrastructure licence conditions:
- Maintain the requirement to provide IPART with a compliance report, audit report and accompanying statement certified by the board detailing the extent to which the network operators have complied with the critical infrastructure licence conditions over the year.
 - Amend the current requirement to provide the audit report to the Commonwealth Representative to a requirement to either provide the documents when requested by the Commonwealth Representative, or at the direction of the Tribunal.
 - Include an additional requirement for the network operators to provide IPART with the report it is required to submit to the relevant Commonwealth regulator under section 30AG of the SOCI Act.

Under the ES Act, IPART is required report to the Minister on the extent to which network operators have complied, or failed to comply, with the licence conditions.^k Self-reported information and audits are key tools we use to assess network operators' compliance with their obligations.

The network operators currently meet this audit requirement each year by engaging a pre-approved critical infrastructure auditor on our audit panel or by nominating an alternate auditor with appropriate expertise. Audits are conducted in accordance with any audit guidelines issued by IPART.^l

i Relevant SOCI obligations – compliance reporting and auditing

The relevant SOCI obligations require network operators to:

1. provide an annual report on the status of its CIRMP as to whether the program is up to date as approved by the board or other governing body.^m
2. notify the Secretary of the Department when there is a notifiable event.ⁿ

We propose to retain the annual critical infrastructure self reports and audit requirement because:

- the SOCI Act does not include an annual audit requirement, and
- it allows IPART to perform our compliance monitoring functions.

^k Section 87(1) of the ES Act.

^l As described in section 2.2.5.

^m Section 30AG(2)(c)&(f) of the SOCI Act.

ⁿ Section 24 of the SOCI Act.

We note the general licence conditions (outside of the critical infrastructure conditions) already contain a "general audit power" allowing IPART to direct the network operators to engage an auditor to conduct an audit at any time as determined by IPART. The intention of this general audit power is to provide additional flexibility to conduct audits on a risk basis.

We consider it is important to maintain an annual audit requirement in addition to our general audit power. The inherent level of risk that these conditions address means that we require a high level of assurance of network operator compliance with these obligations. The purpose and consistent nature of this audit means that a targeted or reduced audit scope is unnecessary and a standing audit obligation reduces the administrative burden associated with ad-hoc audit directions. The process associated with ad-hoc audit directions would place an unnecessary burden on IPART as the regulator and on the network operator without significant net benefit.

Additionally, an annual audit requirement is in line with a number of our licensing principles including being risk-based and consumer outcomes-focused. This is because conditions are expected to be beneficial overall to the availability of the supply of electricity as an essential service.

CyberCX generally recommends maintaining the current compliance reporting and auditing obligations subject to amending the content of the annual compliance report. CyberCX recommends that licence holders provide IPART with a copy of the report they are required to submit to the relevant Commonwealth regulator under section 30AG of the SOCI Act, and that a smaller report be provided for the remaining conditions that are not covered by the SOCI Act.

We propose to not adopt CyberCX's recommendation to receive a smaller report. We consider this may impact our compliance monitoring role and our obligation to report the extent of network operators' compliance to the Minister. This is because receiving the annual SOCI report is not likely to provide IPART with the same level of assurance as an audited report conducted against recognised audit standards. Additionally, there is generally not a complete or direct overlap between the principles-based obligations of the SOCI Act and the more prescriptive licence conditions.

Seek Comment



9. Do you agree with our proposal to retain the compliance reporting and auditing requirements?
10. Are there any additional comments you wish to make on the draft licence conditions or the draft report?

6 Full list of draft recommendations and questions

6.1 Draft recommendations

We have included the full list draft recommendations outlined in this draft report relating to our proposed positions on the current critical infrastructure licence conditions.

Draft recommendations

1.	That the critical infrastructure licence conditions:	16
	<ul style="list-style-type: none"> Retain the requirement that the licence holder must take all practical and reasonable steps to ensure that maintenance of the transmission or distribution system is undertaken solely from within Australia. 	16
	<ul style="list-style-type: none"> Amend the current requirement for the senior officer responsible approve any third party maintenance of the distribution system to instead permit the network operators to acquire, or conduct physical servicing of components from outside Australia, for the purposes of maintenance of the distribution or transmission system where: <ul style="list-style-type: none"> it is not reasonably practicable to acquire the components or conduct physical servicing from within Australia, and the Senior Officer Responsible for Network Operations approves acquisition from, or physical servicing by, a specific person or entity from outside of Australia 	16
	<ul style="list-style-type: none"> Retain the current exceptions to the above requirement where a protocol is established with the Commonwealth regulator. 	17
2.	That the critical infrastructure licence conditions:	19
	<ul style="list-style-type: none"> Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that the system, and all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia. 	19
	<ul style="list-style-type: none"> Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that the requirement that the system is not connected to any infrastructure or network in a way that could enable a person outside Australia to access, control or operate it in whole or in part. 	19
	<ul style="list-style-type: none"> Retain the requirement that the licence holder notify the Commonwealth Representative in advance of any engagement with the market to outsource operation and control of the system. 	19
	<ul style="list-style-type: none"> Retain the exception to the above requirements where a protocol is established with the Commonwealth regulator. 	19
3.	That the critical infrastructure licence conditions:	20
	<ul style="list-style-type: none"> Maintain the requirement for at least two directors to be Australian citizens. 	20
	<ul style="list-style-type: none"> Amend the security clearance requirements, so that at least two directors and any senior officers responsible for operational technology, network operations and security operations must either undertake an AusCheck background check or hold a 	

Negative Vetting Level 1 clearance. Where an AusCheck background check is used, the network operator will be required to reasonably ensure the person does not present a security risk.	20
<ul style="list-style-type: none"> Maintain the exemptions and obligations relating to the timeframes for appointing directors and senior officers responsible in the event of a vacancy subject to amendments to: <ul style="list-style-type: none"> reduce the maximum allowable timeframe from 8 months to 4 months to achieve compliance with obtaining a national security clearance or have undertaken a Background Check following a vacancy include an additional condition enabling the licence holder to nominate a longer exemption period for IPART's approval. 	21
4. That the critical infrastructure licence conditions:	24
<ul style="list-style-type: none"> Maintain the requirement that all Operational Technology Information is held solely in Australia only accessible from within Australia by a Relevant Person who has been authorised by the Licence Holder. Maintain the requirement that Load Data relating to, or obtained in connection with, the operation of the Distribution or Transmission System by a Relevant Person is held solely within Australia, and only accessible from within Australia by a person who has been authorised by the Licence Holder. Maintain the requirement that Third Party Data indirectly accessed or obtained because a Carrier or another person transferred the Third Party Data using the Licence Holder's infrastructure is held solely within Australia, and only accessible from within Australia by a person who has been authorised by the Licence Holder. Remove the requirement that Bulk Personal Data Records are subject to conditions within the licence. 	24
5. That the critical infrastructure licence conditions:	25
<ul style="list-style-type: none"> Maintain the exemptions to the Data Security requirements, Replace the provisions, allowing the Commonwealth Representative or IPART to agree in writing to other arrangements, with a provision enabling the Commonwealth Representative to agree to a Protocol as an alternate to comply with the data security licence conditions. Maintain that existing approvals and arrangements granted or agreed to by IPART or the Commonwealth Representative under the current licences remain in force. 	25
6. That the critical infrastructure licence conditions:	27
<ul style="list-style-type: none"> Maintain the requirement to provide IPART with a compliance report, audit report and accompanying statement certified by the board detailing the extent to which the network operators have complied with the critical infrastructure licence conditions over the year. Amend the current requirement to provide the audit report to the Commonwealth Representative to a requirement to either provide the documents when requested by the Commonwealth Representative, or at the direction of the Tribunal. Include an additional requirement for the network operators to provide IPART with the report it is required to submit to the relevant Commonwealth regulator under section 30AG of the SOCI Act. 	27

6.2 Questions

We have included the full list of questions asked in this draft report relating to the critical infrastructure licence conditions for stakeholder comment below.

Seek Comment

1.	Do you consider the applicable critical infrastructure reporting manual and audit guidelines contain significant issues in complying the requirements in these documents, and if so, what are these issues?	15
2.	Do you agree with our proposal to retain the maintenance of the distribution/transmission system conditions?	18
3.	Do you agree with our proposal to retain the exception to the maintenance condition allowing for a protocol to be agreed with the CISC?	18
4.	Do you agree with our proposal to maintain the requirements for operation and control of the transmission/distribution system?	20
5.	Do you agree with our proposal to amend the security clearance requirements by allowing a network operator to choose between NV1 security clearance or the background checks under the AusCheck scheme?	23
6.	Do you agree with our proposal to retain the data security requirements?	25
7.	Do you agree with our proposal to remove the Bulk Personal Data requirements?	25
8.	Do you agree with our proposal to replace the data agreement provisions with a new provision enabling the Commonwealth Representative to agree to a Protocol?	26
9.	Do you agree with our proposal to retain the compliance reporting and auditing requirements?	28
10.	Are there any additional comments you wish to make on the draft licence conditions or the draft report?	28

© Independent Pricing and Regulatory Tribunal (2024).

With the exception of any:

- a. coat of arms, logo, trade mark or other branding;
- b. photographs, icons or other images;
- c. third party intellectual property; and
- d. personal information such as photos of people.

this publication is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia Licence.



The licence terms are available at the [Creative Commons website](#)

IPART requires that it be attributed as creator of the licensed material in the following manner: © Independent Pricing and Regulatory Tribunal (2024).

The use of any material from this publication in a way not permitted by the above licence or otherwise allowed under the Copyright Act 1968 (Cth) may be an infringement of copyright. Where you wish to use the material in a way that is not permitted, you must lodge a request for further authorisation with IPART.

Disclaimer

This document is published for the purpose of IPART fulfilling its statutory or delegated functions as set out in this document. Use of the information in this document for any other purpose is at the user's own risk, and is not endorsed by IPART.

Nothing in this document should be taken to indicate IPART's or the NSW Government's commitment to a particular course of action.

ISBN 978-1-76049-773-6