IPART Independent Pricing and Regulatory Tribunal | NSW

Review of electricity network operators' critical infrastructure licence conditions

Final Report

May 2025

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
Rosemary Sinclair
Peter Dunphy

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

Tathia Shield Wells	(02) 8226 0218
Matthew van Uffelen	(02) 9113 7789

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 Introduction

1.1 Executive Summary

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

This Final Report sets out our final recommendations for critical infrastructure licence conditions. We outline the justifications and principles we considered in reviewing the licence conditions that we 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 existing critical infrastructure licence conditions establish protections to support supply security and sovereignty, including cyber security.

The existing 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 include at least two Australian citizens and that key personnel pass security vetting and reside in Australia. 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 also protect against significant risks. Left uncontrolled, these risks could manifest themselves with catastrophic consequences. This includes severe and widespread customer impacts such as long-term shutdowns of services that result in significant losses to the NSW economy and significant impacts to other critical infrastructure industry sectors. 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 existing critical infrastructure licence conditions. We recommend 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.

In summary, we recommend largely retaining the existing critical infrastructure licence conditions subject to amendments relating to:

- the ability for senior network operator personnel to obtain background checks as an alternative to obtaining security clearances
- removal of duplicative or related licence obligations covered by Australian privacy legislation
- improved clarity to key concepts (e.g. ICT infrastructure, operational technology and physical servicing).

1.2 Background to the review and critical infrastructure

Under section 77(2)(b) of the ES Act, IPART has 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.

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 rules pertaining to the Risk Management Program under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) were introduced. This was because the changes under the Commonwealth framework may inform the recommendations to the licence conditions.

We commenced our review in 2024 to assess whether the existing critical infrastructure licence conditions are appropriate and for the following reasons:

- Amendments to the SOCI Act recently commenced,[a] which warrant the consideration of the appropriateness 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.

1.3 Summary of review process and timing

On 15 November 2024, we published our draft report and draft licence. We invited stakeholders to provide feedback on our draft recommendations and licence conditions.

Public submissions are available on our web page for this review.[b]

We have now finalised our review of the critical infrastructure licence conditions. A summary of the timeline of our review is below. We have considered all stakeholder input on our draft package, in determining our recommendations.

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

[b] https://www.ipart.nsw.gov.au/review/energy-electricity/review-electricity-network-operators-critical-infrastructure-licence-conditions

This Final Report sets out our final recommendations on the critical infrastructure licence obligations. We have also prepared the full network operator licences, primarily with amendments to appendix containing the critical infrastructure conditions. Additionally, we have made some minor amendments to the body of the licences.

The critical infrastructure appendix sets out our final recommended licence conditions and is intended to replace the existing critical infrastructure appendix in the licences. We recommend changes to the existing licence conditions, and recommend that the Minister vary the licences so that the varied conditions become effective from 1 July 2025.

We provided our recommendations for amended licences to the Minister in May 2025.

The Minister will consider whether to accept our recommendations.

1.4 What we heard from stakeholders about our draft report and licence

We received 7 stakeholder submissions to our draft report including:

- 4 submissions from licensed network operators (Ausgrid, Endeavour Energy, Essential Energy and Transgrid)
- 2 submissions from members of the public
- 1 submission from Anchoram Consulting, a professional services firm.[c]

We heard specific feedback on clarifications and amendments to existing terms and obligations to support compliance with the licence conditions.

We also heard more general feedback on the security landscape of industry including the regulatory, compliance and technological aspects of the critical infrastructure and impacts to their operations. Such comments included:

- the risk management approach as set out in the SOCI Act to mitigate the risks that relate to networks

[c] Submissions from the stakeholders other than the network operators were of a general nature, did not raise specific issues or do not relate to review and as a result, we considered these comments but have not referred to these submissions in this report.

- the impacts of the sovereignty and substantial presence in Australia requirements on the network operator's procurement and supply chain processes
- opportunity for licence conditions to support the energy transition and enable the adoption of new technologies in a cost-effective manner including access to diverse suppliers
- not to impose regulatory burdens and costs on operators that are not reasonable and proportionate.[d]

In response to the general stakeholder feedback, we consider that the advice and input from CyberCX and the Cyber and Infrastructure Security Centree (CISC) into the draft report remains appropriate. We have therefore decided not to recommend substantial changes to the existing licence conditions against these general comments.

This is because based on the advice and feedback from CyberCX and the CISC, we consider the existing licence conditions set a high security standard relative to the risk management approach of the SOCI Act. As a result, we consider the licence conditions should be reassessed at a later review to determine their appropriateness and remain fit for purpose alongside the Commonwealth regulatory framework. This timeframe would also allow the CISC to monitor the effectiveness of the critical infrastructure obligations under the SOCI Act and use this information to inform the future review of critical infrastructure licence conditions.

However, we recommend changes to the draft licence in response to specific feedback on licence conditions issue in order to improve clarification and facilitate efficient compliance. Our changes on the specific issues are outlined in more detail in the relevant chapters.

1.5 How this paper is structured

Chapters 3-6 detail the existing critical infrastructure licence conditions along with our final recommendations. A full list of the recommendations and questions contained in this Final Report are outlined below.

- **Chapter 2** discusses the context for our review and approach, including what critical infrastructure is, what the obligations the existing 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 a minimum number of 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.

[d] Transgrid commented that cost-benefit analysis could be used to determine the reasonableness and proportionality of the condition. Refer to section 2.2.4 for our discussion on cost-benefit analysis.

[e] Within the Commonwealth Department of Home Affairs.

Note, throughout this report we have made references to existing critical infrastructure licence conditions which for simplicity relate to the licence conditions of Ausgrid, Essential Energy and Transgrid only as the licences of Endeavour Energy and ACEREZ differ in licence condition numbers.[f]

For ease of comparison purposes between the existing and recommended licence, a reference to an existing condition excludes the schedule and appendix these conditions appear in (e.g. 1.1) whereas references to the new recommended conditions contain the prefix "B" (e.g. B.1.1).

[f] Endeavour Energy's existing licence contains an additional condition 3.1, relating to foreign operatorship that has been removed as part of this review.

1.6 Final recommendations

We have included the full list of final recommendations outlined in this Final Report relating to our final positions on the existing critical infrastructure licence conditions.

Recommendations

1. That the critical infrastructure licence conditions: 16
   a. 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.
   b. Amend the existing requirement for the senior officer responsible to approve any third party maintenance of the transmission or 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
      - the senior officer responsible for network operations or operational technology approves acquisition from, or physical servicing by, a specific person or entity from outside of Australia.
   c. Retain the existing exceptions to the above requirement where a protocol is established with the Commonwealth Representative.

2. That the critical infrastructure licence conditions: 20
   a. Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that operation and control of system, and all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia.
   b. Retain the requirement that the licence holder use best industry practice for electricity network control systems to ensure that the system is not connected to any infrastructure or network in a way that could enable a person outside Australia to control or operate it in whole or in part.
   c. Retain the requirement that the licence holder notify the Commonwealth Representative (CISC) in advance of any engagement with the market to outsource operation and control of the system.
   d. Retain the exception to the above requirements where a protocol is established with the Commonwealth Representative.

3. That the critical infrastructure licence conditions: 23
   a. Retain the requirement for at least two directors to be Australian citizens.
   b. Amend the security clearance requirements, so that at least two directors and each senior officer responsible for operational technology, network operations or 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, and that a background check has been undertaken in the last 10 years.
   c. Retain the exemptions and obligations relating to the maximum allowable timeframe for appointing directors and senior officers responsible in the event of a vacancy or they cease to meet requirements, subject to including an additional condition enabling the licence holder to nominate a longer exemption period for IPART's approval.

	d. Remove the exemptions and obligations relating to the procedural requirements for appointing directors and senior officers responsible in the event of a vacancy or where they cease to meet requirements and remove the procedural requirements around applying for security clearances.	
4.	That the critical infrastructure licence conditions: a. Retain the requirement that Operational Technology Information is held solely in Australia and only accessible from within Australia by a Relevant Person who has been authorised by the Licence Holder. b. Retain the requirement that Load Data relating to, or obtained in connection with, the operation of the Distribution or Transmission System is held solely within Australia, and only accessible by a Relevant Person, or a person who has been authorised by the Licence Holder. c. Retain the requirement for Third Party Data to be held solely within Australia, and only accessible from within Australia by a Relevant person, or a person who has been authorised by the Licence Holder. d. Amend the requirement for Third Party Data to mean data which the Licence Holder indirectly stores or processes 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 Relevant person, or a person who has been authorised by the Licence Holder. e. Remove the requirements that: – Bulk Personal Data Records – Personal information within Third Party Data are subject to conditions within the licence.	28
5.	That the critical infrastructure licence conditions: a. Retain the exceptions to the Data Security requirements, b. 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. c. Maintain that existing approvals and arrangements granted or agreed to by IPART or the Commonwealth Representative under the current licences remain in force.	32
6.	That the critical infrastructure licence conditions: a. Retain 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. b. Amend the existing 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.	34

2 Context and approach to review

2.1 Critical infrastructure 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 ACEREZ[g].

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 the regulatory framework?

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

The Cyber and Infrastructure Security Centre (CISC) within the Commonwealth Department of Home Affairs also performs certain functions under the existing critical infrastructure licence conditions as the 'Commonwealth Representative'.[i] 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 separate blue shaded boxes throughout this report.

---

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

[h] Section 87(1) of the ES Act.

[i] The Commonwealth Representative is responsible for critical infrastructure security as per the licence, This role is currently performed by the CISC who 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.

2.1.3 What is the intent of critical infrastructure and what obligations are imposed?

The preamble to the applicable network operators' existing 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.

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

- have a substantial presence in Australia, including:
  - various requirements around maintenance, access, operation and control of the transmission or distribution system undertaken within Australia
  - 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 ACEREZ 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.[j]

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.

The ACEREZ licence, which was granted by the Minister in September 2024, contains transitional provisions for the critical infrastructure conditions. These provisions provided time for ACEREZ to establish a protocol with the Commonwealth Representative if necessary to ensure compliance with the critical infrastructure conditions. The time for establishing a protocol has now passed.

We have reviewed the existing transitional provisions and determined that these are no longer necessary to include as part of our final recommended licences. However, we have included a new transitional provision for ACEREZ to allow for the recommended requirement that a network operator's directors undergo a background check or obtain national security clearance (see section 3.3.2 for a discussion of the requirement).[k] This transition provision provides ACEREZ a 4-month grace period (or longer period nominated by ACEREZ and approved by the Tribunal) from the variation date.

2.2 We have summarised how we approached this review

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.

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

[k] ACEREZ's existing licence does not include national security clearance requirements for its directors.

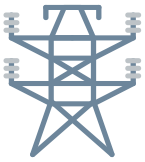
Principle #2: Proportionate and risk-based

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.



Principle #3: Facilitate efficient monitoring and enforcement of compliance

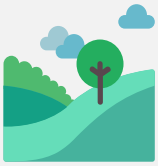
We designed licence conditions that facilitate IPART and co-regulators, such as the CISC, to efficiently conduct their compliance monitoring and enforcement activities on licensed network operators. This includes clearly defined licence, audit and minimum reporting obligations necessary for us to be 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 We engaged an advisor to assist with our review

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

CyberCX has prepared a draft report and supplemental stakeholder submission report[l] both containing recommendations against the existing licence conditions which are referred to in this Final Report.

We engaged CyberCX to review the licensed network operators[m] existing critical infrastructure licence conditions generally applicable to the licensed network operators for the purpose of informing our final recommendations and final 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.

[l] CyberCX, *IPART Cyber Security Licence Conditions Review – Draft Report*, 8 November 2024 and CyberCX, *IPART Cyber Security Licence Conditions Review – Supplemental response*, April 2025. The reports are available on IPART's website.

[m] 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.

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 existing 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 final 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 decided not to adopt its recommendations.

2.2.3 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 existing 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.[n]

2.2.4 Cost-benefit analysis

We did not perform a detailed cost-benefit analysis on critical infrastructure licence conditions. However, we considered the broader cost impacts of a widespread attack on or disruption to the electricity networks involving a large number of customers far outweighs the ongoing costs of regulation.

As outlined in section 2.1.3, the preamble to the existing 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. As a result, the impact from a critical infrastructure incident has the potential to be far reaching. Additionally, an impact to the electricity sector would also cause a significant impact to other critical infrastructure sectors which depend on electricity. Therefore, the costs are difficult to quantify as the magnitude would depend on a number of factors such as the nature, duration and severity of an incident.

We also consider most of the substantial costs to achieve compliance with the critical infrastructure conditions associated with the establishment of IT systems and network security have already been incurred. This is because the licence conditions have been in effect for many years following the lease of the NSW electricity networks, and as a result, future costs are more likely to be driven by maintaining ongoing compliance. Additionally, we have not recommended new substantial requirements, but have made improvements to requirements that assist network operators to achieve compliance more efficiently thereby reducing the costs of regulation.

As the Minister must impose conditions on maintaining a "substantial operational presence in Australia", our licence recommendations are intended to meet this regulatory requirement. We consider the conditions are therefore necessary to safeguard against threats and ensure the security of the network.

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.

[n] Please refer to section **Error! Reference source not found.** for an overview of the existing obligations under the 'Substantial presence in Australia' requirement.

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 considered the reporting manual and the audit guidelines and decided that it was not necessary to consult on these documents as part of this review. This is because these documents outline general process and timing requirements in relation to the conduct of audits and reporting on a network operator's compliance with the critical infrastructure conditions. We will amend these documents at a later date to ensure the requirements under these documents are consistent with any associated final licence conditions prior to the licence conditions taking effect.

2.3 We have improved the clarity of the conditions

We consider the existing critical infrastructure licence conditions within the Ausgrid, Endeavour Energy, Essential Energy and Transgrid licences could be more clearly articulated. We have made plain English and structural changes to these final 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.

As we have applied the structural and readability changes throughout the final licence, for brevity, we have not referred to each of the individual wording changes specifically in each of the recommendations in this report. 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".[o]

The existing licence conditions require work to be conducted, information to be retained, and control to be accessible from within Australia. The conditions also require that boards or governing bodies contain a minimum number of 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 requirements (existing condition 1.1)

Final recommendation

1. That the critical infrastructure licence conditions:
   a. 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.
   b. Amend the existing requirement for the senior officer responsible to approve any third party maintenance of the transmission or 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

[o] ES Act, Sch 2 clause 6(5)(c).

- the senior officer responsible for network operations or operational technology approves acquisition from, or physical servicing by, a specific person or entity from outside of Australia.

c. Retain the existing exceptions to the above requirement where a protocol is established with the Commonwealth Representative.

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 Act[p] 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.

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.

3.1.1 We recommend largely retaining the existing maintenance obligations

We maintain our draft position to retain the existing maintenance obligations but recommend including new definitions to provide further clarification to key terms.

Stakeholder responses included:

- Ausgrid commented that it seeks clarity around physical servicing of components and that it should not apply to components that are taken off the system (e.g. for warranty, investigations etc) and are not returned to service on the System. Ausgrid recommended that "Components" in this context should be defined to not include maintenance of primary assets that do not contain active equipment.

[p] Including related requirements such as the Risk Management Program Rules.

- Ausgrid also commented that it recommends the senior officer responsible for approving the acquisition from, or physical servicing could be expanded to include the senior officer with operational technology responsibility.
- Endeavour Energy commented that the definition and boundaries of "transmission or distribution system" should be clearly articulated.
- Endeavour Energy commented that the draft position on virtual servicing could be updated to articulate specific carve-outs or circumstances.
- Transgrid agreed with our proposal to retain the existing requirements for maintenance of the distribution/transmission system.

We note the existing 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 imply 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 have clarified our position in the recommended condition B.2.2(a) to permit the acquisition, or physical servicing of physical 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 or operational technology has approved the acquisition or physical servicing by a specific person or entity.

We have responded to stakeholder comments by largely adopting CyberCX's new recommended definition for "components" in its supplemental report. We have defined "components" in the recommended licence to mean "any part of the transmission or distribution system that contains electronic processor capabilities, electronic storage of data or communications capability". We have also added a new definition for "physical servicing" to clarify that the physical servicing of components includes such items that are removed and reinstalled.

In response to Ausgrid's comment, we have made provisions in the recommended condition B.2.2(b) for the senior officer with responsibility for Network Operations, in addition to the senior officer with responsibility for operational technology, to approve the acquisition or physical servicing of components outside of Australia.

We have not decided to expand the definition or boundaries of a distribution system or a transmission system. This is because such systems are already broadly defined in ES Act. Instead, we consider our new definitions to several key terms in the licence provide additional clarity around the scope of the requirements.

CyberCX in its draft report 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 have decided not to adopt CyberCX's recommendation to provide provisions for virtual servicing and not include specific carve-outs circumstances where virtual servicing would be permitted as suggested by Endeavour Energy. 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, particularly from overseas, arising from increased access.

The CISC agrees with our 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.

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 high risk operational information from outside Australia.

We acknowledge the substantial presence requirements may impose restrictions on local activity and access to expertise and so we recommend maintaining the existing exemption requirements. As a result, network operators may enter into a Protocol with the Commonwealth Representative (i.e. the CISC) under recommended condition B.1 to agree on 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.

While we have allowed for exceptions to the conditions through the establishment of a protocol, we have not provided further guidance or specified the processes to engage with the CISC. In line with our licensing principles, we consider that conditions where possible should be outcomes-focused rather than contain prescriptive or process-based conditions, and therefore the licence need not specify a process for arranging protocols with the CISC. We consider this approach achieves the necessary outcome of involving the CISC in assessing the risk of any proposed deviation from the standard licence conditions and approving the deviation if it considers the risk can be appropriately managed with suitable controls in place.

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 network operators.

The recommended licences also include a new requirement for network operators to provide IPART with a copy of the new or varied protocol upon finalisation with 14 days. This new requirement provides IPART with visibility of which conditions and network operators are subject to arrangements with the CISC. This would also assist in auditing these requirements.

3.2 Access, operation and control of the transmission/distribution system requirements (existing condition 1.2)

Final recommendation

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

The conditions provide protections around 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 of a protocol with the Commonwealth Representative.

These obligations ensure that:

- the network operators have appropriate controls in place to prevent the operation and control of the transmission/distribution system and associated ICT infrastructure from being accessed, operated and controlled from outside of Australia and therefore they help to support the security and availability of the network.
- Prevent connections to other infrastructure which could control or operate 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.

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 recommend retaining the requirements for the access, operation and control of the transmission/distribution system

We maintain our draft position to retain the existing obligation that, except where allowed for under a protocol, a network operator must ensure the operation and control (as required) of its transmission/ distribution system from within Australia.

Stakeholder responses included:

- Anchoram Consulting commented further explanation of 'best industry practice' should be provided by referring to relevant sources of authority, industry specific standards or to remove that wording in preference of an alternative.
- Essential Energy commented on the inclusion of the word "access" in the draft licence conditions requiring the Licence Holder to ensure its system could prevent a person outside of Australia to access, control or operator the system. Essential Energy commented that "access" is not included in the existing condition.
- Essential Energy requested clarification around the phrase "associated ICT infrastructure". Essential Energy considers this should refer to software and systems used in the operation and control of the network infrastructure used for the conveyance of electricity.
- Transgrid agrees with IPART's proposal to retain all the existing requirements for operation and control of the transmission/distribution system. TransGrid also commented that the existing licence condition requiring a licence holder to ensure that its 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, is unnecessary and duplicative.
- Endeavour Energy commented that "Best Industry Practice" is defined in the existing and draft licence conditions as including "access required by relevant Australian regulators and market system operators" but the definition does not otherwise include any underlying conceptual guidance as to what would be captured by the definition.

In response to Essential Energy's comment relating to access, we have not included the word access in recommended condition B.2.3(b) which was included in the draft licence. As our final position is to retain the existing condition. we agree with Essential Energy and have aligned the wording in the final condition to better reflect the existing condition.[q]

CyberCX's draft 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 therefore consider retaining the operation and control requirements to be important for supporting supply security and sovereignty, including security over the malicious activities from external and unauthorized control of the network.

[q] We note that the word "access" appears in ACEREZ's operating licence 1.2(b). We have removed this term in the recommended ACEREZ licence to ensure consistency with the other licensed network operators.

We agree that the phrase "associated ICT infrastructure" in the existing licences require clarification and acknowledge the potential interpretation that all ICT infrastructure is subject to the requirements. Without further specification, associated ICT infrastructure could unintentionally capture a broad range of administrative activities and could be misunderstood or inconsistently interpreted by other network operators or auditors.

In response to the stakeholder feedback, we consider clarifying the scope of the associated ICT infrastructure is necessary to ensure network operators can achieve compliance with the licence conditions. As a result, we consider that only ICT infrastructure that directly supports the operational technology environment should be subject to the requirements. We have adopted CyberCX's recommended definition in its supplemental report for ICT infrastructure.

However, we have not made changes to address Transgrid's comments that some conditions may be duplicative, as we consider the conditions provide an additional level of protection to the system. We therefore maintain CyberCX's draft report recommendation to retain the access and control requirements.

We have decided not to further specify the term "best industry practice" and have removed the definition from the draft licence relating to managing control of a transmission/distribution network. This is because the network operators currently achieve this licence requirement using a variety of different controls, standards and frameworks. This 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.

In the absence of a definition for this concept in the licence, the term would have its ordinary and natural meaning having regard to its context and purpose. The term best industry practice infers the adoption of generally accepted principles, prevailing network operator practices and achievement of expected outcomes in order to support high standards of security. It may include the application of relevant industry standards and employment of specialist expertise.

3.2.2 We recommend retaining the notification and protocol requirements with the Commonwealth Representative

We maintain our draft position to retain the notification and protocol requirements.

Essential Energy commented that it agrees with retaining the operational and control requirements subject to protocols being in place. This is because protocols allow for emergencies where direct vendor support may be necessary as a last resort.

Essential Energy agrees on the criticality of operation and control of its network being undertaken only from within Australia or in line with a Protocol agreed with the Commonwealth Representative.

Given the stakeholders did not raise any issues with the notification and protocol requirements in relation to operation and control of the systems, we consider it is appropriate to retain the existing requirements in recommended conditions B.1 and B.2.4.

3.3 Australian citizenship and security clearance requirements (existing conditions 1.3-1.5)

Final recommendation

3. That the critical infrastructure licence conditions:
   a. Retain the requirement for at least two directors to be Australian citizens.
   b. Amend the security clearance requirements, so that at least two directors and each senior officer responsible for operational technology, network operations or 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 to the operation and control of the System, and that a background check has been undertaken in the last 10 years.
   c. Retain the exemptions and obligations relating to the maximum allowable timeframe for appointing directors and senior officers responsible in the event of a vacancy or they cease to meet requirements, subject to including an additional condition enabling the licence holder to nominate a longer exemption period for IPART's approval.
   d. Remove the exemptions and obligations relating to the procedural requirements for appointing directors and senior officers responsible in the event of a vacancy or where they cease to meet requirements and remove the procedural requirements around applying for security clearances.

As outlined previously, the ES Act requires the Minister to impose licence conditions for maintaining 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 existing conditions require licence holders to have at least two directors who hold Australian citizenship and any senior officers responsible for operational technology, network operations or security operations, to reside in Australia. Additionally, the conditions require the two directors and any senior officers responsible to hold a national security clearance, being a clearance of not less than Negative Vetting Level 1 (NV1) (or equivalent) issued by the Australian Government Security Vetting Agency (AGSVA).

The existing conditions also provide temporary exemptions to the above requirements for the purposes of appointing directors and senior officers and applying for NV1 security clearance where a person vacated their position or a ceased to satisfy the above requirements.

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 recommend retaining a citizenship requirement

We maintain our draft position to retain a citizenship requirement for at least two directors to be Australian citizens.

We consider that a citizenship requirement in the recommended condition B.2.5(a) 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 understand other frameworks may also have citizenship requirements and that this reduces the burden of this condition. For example, 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 recommend amending the security clearance requirements for senior officers and directors

We maintain our draft position to amend the security clearance requirements for senior officers and directors. These personnel must either obtain NV1 security clearance or undertake an AusCheck background check.

Stakeholder responses included:

- Essential Energy and Transgrid support the flexibility allowing a network operator to consider using AusCheck background check, however, Essential Energy notes that it would continue to obtain security clearances due to the need to receive important cyber security information.

- Ausgrid does not agree with our draft recommendation to allow network operators to choose between NV1 security clearance or the background checks under the AusCheck scheme. Ausgrid commented that NV1 security clearance is important for key roles being able to receive important security information from Commonwealth agencies.
- Ausgrid does not support the draft requirement that it must ensure that a director does not present a security risk due to the manner in which Ausgrid's directors are appointed by its shareholders. Ausgrid commented that its directors are appointed at the discretion of its shareholders under the terms of the partnership deed and therefore it does not have the ability to "ensure" or enforce a licence condition that pertains to Directors.

Overall, 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 draft 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 existing NV1 security clearance requirements.

Although CyberCX recommended the AusCheck background checks could replace the NV1 security clearance requirements, our draft recommendation was to allow the licensees' key personnel undertake AusCheck background checks as an alternative to obtaining NV1 security clearance. This provides network operators additional flexibility.

We have decided to maintain our draft position in the recommended licence conditions B.2.5(c) and B.2.7(b) and consider that allowing a network operator to have the flexibility to choose between undertaking an AusCheck background check or NV1 security clearance is appropriate. 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. Also maintaining the NV1 security allows the network operator's key personnel to continue to receive important security information from government agencies.

In making our recommendation we considered comments that 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. We have also made amendments to the timeframes for obtaining security clearances (see section 3.3.3) to address this concern.

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 recommended amendment to also allow for an AusCheck background check, reduces the regulatory burden and is consistent with our licensing principles to protect consumers while also being proportionate. On balance we consider allowing additional flexibility does not significantly increase the risks and supports efficient compliance with licence conditions. 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.

In order to further balance any increased risk from providing for AusCheck to replace NV1 clearances, we recommend retaining our draft position that the licence holder is to reasonably ensure that any person subject to an AusCheck is not a security risk under recommended condition B.2.9. 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 high risk information or critical assets.

We note Ausgrid has raised a concern regarding their ability to "ensure" or enforce an outcome of directors not presenting a security risk, highlighting that appointing directors is subject to governance requirements (draft condition 2.1). However, we recommend retaining the draft condition. Although we acknowledge that network operators may be subject to specific governance arrangements around the appointment of directors, we maintain our initial view that key personnel who hold a degree of strategic influence over the business present a higher risk and must be subject to a higher level of scrutiny by network businesses. Furthermore, Ausgrid retains the option to obtain an NV1 national security clearance for its directors instead of an AusCheck, consistent with its current licence, to avoid impacting compliance with the proposed condition B.2.9.

To further strengthen the security requirements, we have recommended that the licence condition B.2.5 require that a background check should be subject to a 10 year renewal/validity period to align with equivalent period set by AGSVA for an NV1 security clearance to ensure consistency of these requirements and that these security checks remain up to date.

In response to feedback on the draft definition of National Security Clarance, we have removed the reference to the NSW Government involvement in issuing security clearances to reflect that security clearances are instead issued by AGSVA and not the NSW Government. 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. As a result, the application process may require involvement from the NSW Government however we have not specified the process for applications in the licence.

3.3.3 We recommend largely maintaining the requirements on appointing directors and senior officers in the event of a vacancy

We maintain our draft position that the licence impose maximum timeframes to achieve compliance with the above director and senior officer requirements in the event of a vacancy in these positions, or a person ceases to meet the requirements (i.e grace period).

Stakeholder responses included:

- Endeavour Energy commented that the existing 8-month timeframe to obtain NV1 security clearance should be retained.
- Transgrid also commented that it has experienced processing delays with this requirement.

We acknowledge Essential Energy and Transgrid's comments that NV1 security clearances may be impacted by delays due to processing times outside the direct control of the network operator. As a result, we have amended our draft requirements to instead retain the timeframe in existing condition 1.5(c) such that recommended conditions B.2.6(b) and B.2.8(b) allow for an 8-month timeframe to achieve compliance with the security clearance requirements. Additionally, these recommended licence conditions include an additional provision enabling the licence holders to nominate a longer period for IPART's approval if necessary.

We have retained our drafting changes and simplifications to the requirements to improve clarity, while maintaining the intent of these conditions,

4 Data security

4.1 Holding information and data within Australia requirements (existing conditions 2.1 & 2.4)

Final recommendations

4. That the critical infrastructure licence conditions:
   a. Retain the requirement that Operational Technology Information is held solely in Australia and only accessible from within Australia by a Relevant Person who has been authorised by the Licence Holder.
   b. Retain the requirement that Load Data relating to, or obtained in connection with, the operation of the Distribution or Transmission System is held solely within Australia, and only accessible by a Relevant Person, or a person who has been authorised by the Licence Holder.
   c. Retain the requirement for Third Party Data to be held solely within Australia, and only accessible from within Australia by a Relevant person, or a person who has been authorised by the Licence Holder.
   d. Amend the requirement for Third Party Data to mean data which the Licence Holder indirectly stores or processes 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 Relevant person, or a person who has been authorised by the Licence Holder.
   e. Remove the requirements that:
      - Bulk Personal Data Records
      - Personal information within Third Party Data

      are subject to conditions within the licence.

The existing conditions contain restrictions on the management of certain types of information, such as operational technology information, load data, bulk personal data, and third party data. These restrictions manage where the information is held and how it is accessed to reduce the risk of unauthorised access to sensitive or critical information.

Relevant SOCI obligations – Data security

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

Relevant SOCI obligations – Data security

- 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 recommend retaining the operational technology requirements

We maintain our draft position to retain the existing requirement that operational technology information and associated ICT infrastructure of the operational network is held solely in Australia and access to such information is authorised. We also recommend including additional definitions to operational technology/information to improve clarity.

Stakeholder responses included:

- Endeavour Energy commented that operational technology should be defined to ensure consistency in interpretation and application. Endeavour Energy suggested that the definition relate to technology that directly controls devices on the distribution system and transmission system.

In response to stakeholder comments, we agree that operational technology should be defined to improve interpretation. As a result, the recommended licence includes a new definition of operational technology and operational technology information.

CyberCX in its supplemental report, recommended that the definition of operational technology should not be limited to the control of network systems as this would exclude monitoring. As a result, we have largely adopted CyberCX's recommended definition so that operational technology relates to technology that controls or monitors devices on the system.

Overall, we consider that the security of operational technology information is of critical importance to protect the transmission/distribution system against malicious attacks by bad actors. This type of 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 and protection from foreign exploitation of system vulnerabilities. This is because storing, transmitting, or processing sensitive operational information outside Australia increases the risks of loss of control of information due to increased attack pathways. We consider that retaining the information and restricting access to within Australia reduces this risk. In addition, surveillance and enforcement activities by Australian security agencies are more likely to be effective from activities within Australia, providing additional protection from unauthorised access.

4.1.2 We recommend retaining requirements to hold load data within Australia

We have maintained our draft position to retain the information and data requirements subject to additional clarifying amendments to key terms. We have also made amendments to the data security condition for load data to better align with the intent of our draft recommendation.

Stakeholder comments included:

- Ausgrid commented that the draft data security licence condition brings additional onshore access requirements for load data and do not reflect IPART's draft recommendations or CyberCX analysis.
- Endeavor Energy commented that although it supports maintaining the storage of load data and third party data within Australia, limiting access solely within Australia would not be feasible for its operations (see section 4.1.4 for our recommendations on third party data).
- Endeavour Energy commented it does not support the proposal to integrate the data security requirement under the new single term "sensitive information" as this may give rise to confusion, with existing classifications such as "Business Critical Data" under the SOCI Act and Endeavour Energy's own internal classification.
- Endeavour Energy commented that it may not be able to comply with draft licence conditions as several of its critical applications that process load data or third party data currently rely on overseas support.
- Essential supports our proposal to retain the data security requirements.
- Transgrid commented that it agrees that the security of critical information is of utmost importance to protecting the transmission system against attacks. However, Transgrid commented that the requirement that such data only be accessible from within Australia is unnecessarily restrictive and is creating inefficiencies in its procurement and supply chain processes.

The draft licence condition for data security required load data to be held within Australia and only accessible from within Australia by a person who has been authorised. We note that this does not align with the existing licence condition 2.1(b)(i), as while the existing condition requires the data be held in Australia, it does not require that access only occur from within Australia.

We have responded to the stakeholder comments by removing the additional access requirement imposed on load data from the draft licence condition to better reflect the requirement of the existing condition. We have also amended the draft condition relating to who is authorised to access the data to reflect the existing conditions. As a result, our amendments better align with our intent to retain the existing data security conditions.

In the final recommended licence conditions under B.3.1, we have consolidated a number of the existing data security licence conditions requiring certain information be held and accessed within Australia. As a result, the final recommended licence refers to operational technology, load data and third party data under the single term 'secure data' whereby such information is required to be held and accessed in Australia.

4.1.3 We recommend removing the requirements for Bulk Personal Data Records

We maintain our draft position to remove the requirements for Bulk Personal Data (existing condition 2.1(b)(ii)).

Stakeholder responses from Anchoram Consulting, Ausgrid, Endeavour Energy, Essential Energy and Transgrid supported the removal of the requirements around Bulk Personal Data records from the licence as the existing licence conditions duplicate Australian privacy legislation.

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.[r] 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 in 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) provide sufficient protection. We therefore consider the licence requirements around Bulk Personal Data Records to be duplicative and unnecessary.

As outlined in the section below, we have also removed the related privacy requirement for third party data for certain uses and management of personal information to ensure consistency with our draft and final positions on privacy requirements.

4.1.4 We recommend amending the third party data requirements

We have amended our draft position of maintaining the third party data requirements and have made changes in recommended conditions to improve interpretation and better align with our approach to related privacy legislation obligations.

Stakeholder responses included:

- Essential Energy commented that the licence is unclear whether third party data; includes all types of third party data, is data obtained in connection with the operation of the distribution system, or includes customer and other external supplier or retailer data. Additionally Essential Energy queried what is meant by a licence holder "indirectly" obtaining or accessing third party data.
- Endeavour Energy does not support limiting access to third party data solely within Australia.
- Endeavour Energy also commented third party data requirements on personal identifiable information is potentially out of IPART's scope given our other licence recommendations to remove related privacy legislation obligations such as bulk personal data requirements.

We agree with Endeavour Energy and consider that we should approach privacy obligations consistently. As a result, we recommend removing personal information from the definition of third party data to better align with our licence recommendations to remove bulk personal data requirements (as outlined in 4.1.3 above).

[r] Section 15 of the Privacy Act.

We have also amended the definition of the third party data (within the definition of secure data) by adopting CyberCX's proposed definition in its supplemental response. CyberCX recommended that the third party data obligations apply to data which is stored or processed instead of data which it obtains and accesses. We consider this amendment provides clarification and limits the scope of third party data captured by the licence condition to data which is in the control of the network operator.

4.2 Exceptions for complying with data security conditions (existing condition 2.2)

Final recommendations

5. That the critical infrastructure licence conditions:
   a. Retain the exceptions to the Data Security requirements,
   b. 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.
   c. Maintain that existing approvals and arrangements granted or agreed to by IPART or the Commonwealth Representative under the current licences remain in force.

The licence conditions contain exceptions to the data security requirements which allow a network operator or a relevant authorised person to disclose, hold, use or access the information or data referred to above in specified circumstances.

4.2.1 We recommend retaining exceptions for complying with data security conditions

We maintain our draft position and recommend substantially retaining the existing exceptions under existing condition 2.2 subject to some amendments.

Stakeholder responses included:

- Ausgrid commented that "best industry practice" should be removed from the licence to avoid conflicting interactions with other regulatory requirements.
- Endeavour Energy requested clarification on the term "best industry practice". Endeavor Energy queried a potential inconsistency between the draft definition of "best industry practice" and the existing exception allowing information to be disclosed "in the ordinary course of business and in accordance with *good* electricity industry practice".
- Ausgrid and Endeavour Energy supported an exemption process enabling the Commonwealth Representative to agree to a Protocol. However, Endeavour Energy considers that it should be limited to operational technology information. Load data and third party data access should be reconsidered.

In response to stakeholder comments, we have removed the definition of the term "best industry practice" where the draft licence permits access by relevant Australian regulators and market and system operators to better reflect the existing licence requirements. We agree with Ausgrid that the definition is unnecessary in this case. This is because the regulatory requirements such as the National Electricity Rules already govern information exchanges for the operation of the wholesale electricity market and also govern the exchange with economic regulators.

However, we consider the term "good industry practice" of the existing licence condition 2.2(d) may cause some confusion over the required level of standard or expectation. As a result, we have amended the term to "best industry practice" for consistency with other licence conditions that use the term. In this instance, the licence relies on the ordinary meaning of the term and the practices of other regulations to govern the information exchange mechanisms and requirements.

Overall, we consider most of the data security exceptions included in condition B.3.2 of the recommended licence are necessary. From time to time a network operator, or a third party is required to disclose, hold, use or access the type of information referred to in the previous section for legitimate reasons such as legal, regulatory, industry, financial or other reasons. The appropriate use of such information as described in the licence represents a low risk to data security and contributes to the effective and efficient operation of the network business.

We recommend replacing two of the existing exemptions (existing conditions 2.2(f) and 2.2(g) with an expanded protocol (recommended conditions of B.1) referenced in the substantial presence in Australia conditions discussed in section 3 of this report. The two existing exemptions relate to approvals given by either IPART or arrangements agreed to by the Commonwealth Representative. For consistency, we recommend that all new or varied protocols are to be entered into with only the Commonwealth Representative (as performed by the CISC), as we consider the CISC is the appropriate organisation to assess the risks and approve any deviations from the licence conditions. 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.

This Protocol may also cover items in other parts of the licence including network maintenance and network operation and control. 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. We note any pre-existing arrangements will continue to be valid and do not have to be incorporated into the protocol.

5 Compliance reporting and auditing

5.1 Compliance, reporting and auditing conditions (existing condition 3)

Final recommendations

6. That the critical infrastructure licence conditions:
   a. Retain 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.
   b. Amend the existing 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.

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.[s] 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.[t]

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.[u]

2. notify the Secretary of the Department when there is a notifiable event.[v]

[s] Section 87(1) of the ES Act.
[t] As described in section 2.2.4.
[u] Section 30AG(2)(c)&(f) of the SOCI Act.
[v] Section 24 of the SOCI Act.

5.1.1 We recommend retaining the requirement to provide an audit report and compliance statement

We have maintained our draft position on the requirement to provide an annual audit report and compliance statement against the critical infrastructure licence conditions.

Stakeholder responses included:

- Ausgrid and Essential Energy supported these auditing and reporting requirements.
- Transgrid supports the audit requirements as it considers the audits are an effective and independent mechanism to provide the necessary assurance compliance with its licence obligations.

We recommend retaining the existing IPART annual critical infrastructure self reports and audit requirements under existing conditions 3.1-3.4 because:

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

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 preparing and issuing 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.

5.1.2 We recommend removing the draft requirement to provide the annual SOCI report

We have amended our draft position requiring network operators to provide IPART a copy of the annual report that they are required to submit to the CISC under the SOCI Act.

Stakeholder comments included:

- Transgrid commented it does not support the recommendation to provide IPART with a copy of the report that it is required to provide to the CISC as IPART is not an entity to whom protected information may be disclosed under section 43E of the SOCI Act.

- Endeavour Energy supported CyberCX's draft recommendation to provide the two forms of annual reports required by IPART and under the SOCI Act, as it considers it would be more efficient and avoid duplication.

CyberCX in its draft report generally recommended maintaining the existing compliance reporting and auditing obligations subject to amending the content of the annual compliance report. CyberCX recommended 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 IPART audit report be provided for the remaining conditions that are not covered by the SOCI Act.

In response to Transgrid's comments, we agree that the SOCI Act may preclude IPART from receiving the information within the annual report under the SOCI Act directly from the network operators.

As a result, we also maintain our draft position to not adopt CyberCX's draft recommendation to receive a smaller IPART audit 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 we consider receiving the annual SOCI report (if permissible under the SOCI Act) 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.

We therefore recommend removing the draft licence condition requiring the network operator to provide IPART with the annual SOCI report.

ISBN 978-1-76049-802-3