



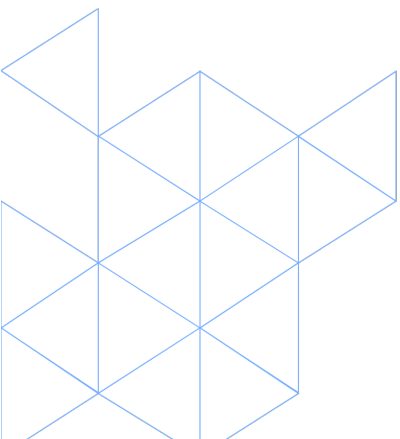
IPART Cyber Security Licence Conditions Review

Draft Report

Prepared by CyberCX on behalf of
NSW Independent Pricing and Regulatory Tribunal (IPART)

DATE: 8 November 2024

Lead Author: Lachlan McGrath | Manager – Strategy & Consulting



Key Details

Project Details

Client Details	
Client Name	IPART
Client Contact	Jonathan Hopson

Table 1 - Project Details

Contacts for Enquiries

Please direct any enquiries to the following contact:

CyberCX Contacts	
Name	Lachlan McGrath
Role	Manager – Strategy & Consulting
Phone	+61 407 103 881
Email	lachlan.mcgrath@cybercx.com.au

Table 2 - CyberCX Contact Details

Contents

- 1 Executive Summary 5
- 2 Context and Background 8
 - 2.1 Background8
 - 2.2 Document Scope8
 - 2.3 Not Legal Advice9
 - 2.4 Threat Landscape9
 - 2.5 IPART’s Recommended Risk Tolerance 11
- 3 Intended Outcomes..... 12
 - 3.1 What are critical infrastructure regulations trying to achieve?..... 12
 - 3.2 Intended outcomes of the SOCI Act and CIRMP Rules 12
 - 3.3 Intended outcomes of Electricity Supply Act Licence Conditions..... 13
- 4 Findings..... 15
 - 4.1 Regulatory Interplay..... 15
 - 4.2 Regulatory Authority over the Security of NSW Electricity Assets..... 15
 - 4.3 Possible Impact on Regulatory Compliance..... 16
 - 4.4 Reduced Security Requirements in some areas.....17
 - 4.5 IPART Could Maintain Most Licence Conditions.....17
 - 4.6 Response from the Department of Home Affairs..... 18
 - 4.7 Overlapping Conditions20
 - 4.7.1 Overlapping Conditions - Data Security20
 - 4.8 Amend conditions22
 - 4.8.1 Amend Conditions - Substantial Presence in Australia22
 - 4.8.2 Amend Conditions - Data Security.....28
 - 4.8.3 Amend Conditions - Compliance 31
 - 4.9 Retained Conditions.....32
 - 4.9.1 Independent Conditions - Substantial Presence in Australia32
 - 4.9.2 Independent Conditions - Data Security36
 - 4.9.3 Independent Conditions - Compliance.....37
- Appendix A Endnotes39



Tables

Table 1 - Project Details2

Table 2 - CyberCX Contact Details.....2

Table 3 - Overlapping Conditions - Data Security in Australia 21

Table 4 - Amended Conditions - Significant Presence.....26

Table 5 - Amend Conditions - Data Security.....30

Table 6 - Amended Conditions - Compliance..... 31

Table 7 - Independent Conditions - Substantial Presence in Australia.....35

Table 8 - Independent Conditions - Data Security 37

Table 9 - Independent Conditions - Compliance.....38

DRAFT

1 Executive Summary

There is overlap between the cyber security obligations set at the federal and state levels. This reflects the similarity in the objectives of the Electricity Supply Act and licence conditions administered by IPART; and the *Security of Critical Infrastructure (SOCI) Act*, administered by the Department of Home Affairs. Both have the primary outcome of preserving the security and availability of Australia's critical infrastructure.

Within this context, the SOCI framework establishes a principles-based obligation on critical infrastructure providers to manage 'material risk' across four hazard domains¹ through a critical infrastructure risk management program (CIRMP). Material cyber risk is defined to include a stoppage or major slowdown of critical infrastructure assets, as well as the offshore storage, processing and access to sensitive data or systems. Operators of 'systems of national significance' as declared by the Minister for Home Affairs may also become subject to 'enhanced cyber security obligations'.

Licence conditions set and administered by IPART within scope of this report include:


- ▶ Substantial Presence in Australia,
- ▶ Data Security, and
- ▶ Compliance.

Relevantly, the IPART licence conditions are more prescriptive than the principles set by the SOCI-framework and afford operators of relevant assets a greater level of precision in the expectations of government in preserving the security of NSW's electricity supply.

Consistent with IPART's licence condition principles, the Australian Government's Deregulation Agenda and Regulator Performance Guide², and section 30AH(6)(a) of the SOCI Act, IPART is seeking to harmonise IPART licence conditions with the SOCI Act framework and other regulatory requirements. To achieve this, IPART is undertaking an independent review of licence conditions in the context of the security landscape of the network operators and the broader regulatory framework. The intended outcome is to improve regulatory outcomes and minimise any regulatory burden where appropriate. This report aims to outline the overlapping licence conditions and suggest amendments to licence conditions. Factors taking into consideration were the:

- ▶ Preservation of the security of NSW's electricity supply,
- ▶ Desirability of harmonisation between federal and state obligations,
- ▶ Information required by the NSW Government to determine and have confidence that the security of its electricity supply is appropriately managed,
- ▶ the authorities and capabilities the NSW Government requires to intervene if required to ensure its expectations of electricity supply security are met,
- ▶ Maturity of federal and state regulatory authorities and level of resources available to oversee regulated entities,
- ▶ Benefits and shortcomings of principles-based regulation and balanced against the prescription of minimum requirements,
- ▶ Cost of regulation and the impact on regulated entities, and
- ▶ Practicality of regulated entities meeting their regulatory obligations, especially with respect to operational technology and the adoption of new technologies across the electricity network.

IPART's licence conditions will continue to interact with related regulatory requirements including the SOCI Act and Privacy Act. IPART's licence conditions should reflect the full



regulatory environment experienced by licence holders and should be comfortable in both; relying on more appropriate regulatory requirements to achieve certain security outcomes, and crafting licence conditions to supplement other regulatory requirements that do not fully satisfy IPART's risk appetite.

CyberCX's preliminary view is that a revision of IPART licence conditions to provide regulated entities greater fidelity on the steps they must take to manage their cyber risk under the SOCI framework is the most effective way of harmonising federal and NSW government requirements.


Under this approach, the more prescriptive conditions set by the NSW government should recognise the benefit of accessing offshore technology and capabilities, while maintaining a level of assurance that associated risks have been identified and managed. A key area of focus should be setting expectations for the management of third parties with respect to the operation and maintenance of SCADA systems. In circumstances where the offshore processing of data is unavoidable, conditions geared towards ensuring awareness of where data is transmitted and controls in place to maintain the availability of key systems represent a minimum baseline. A similar approach should govern the provision of remote support and the management of access. Both would be consistent with the broader approach to data sovereignty of the federal government approach reflected in its Hosting Certification Framework³.

To this end, there may also be scope to compel changes in vendors' arrangements through the imposition of revised licence conditions. These could include forbidding offshore access to operational systems in Australia, forbidding the onforwarding of access to high-risk locations, and forbidding the passage of data through high-risk locations. The intended outcome would be the establishment of local vendor capability to host relevant data on vendor systems that is provided by regulated entities and then used by vendors to leverage their offshore footprint to provide support.

For example, licence holders or vendors would set up a test environment separated from the actual operational environment; the licence holder would move data into this environment and have the vendor's overseas experts access this segregated test environment to undertake their assessment. This would allow licence holders to leverage overseas experts without increasing risk to the operational environments of their electricity infrastructure.

In summary, this report found that:

- ▶ Some (1/11) of the Substantial Presence in Australia licence conditions could be removed and another (1/11) amended, 9/11 should be retained in their current state
 - ▶ Most of these should be retained because remote access is a significant risk to electricity infrastructure.
 - ▶ The language of one of the licence conditions related to accessing data and systems from outside Australia (s1.1a) is no stronger than the SOCI Act Critical Infrastructure Risk Management Program. This licence condition should be removed.
 - ▶ The licence conditions related to corporate structure and ownership remain relevant and should be retained as they are.
- ▶ Some (2/13) of the Data Security licence conditions could be removed, and others (2/13) could be amended. The remaining 9/13 should be retained as they are.
 - ▶ While many of the intended outcomes of all these licence conditions fall within the requirements of the SOCI Act Critical Infrastructure Risk Management Program (CIRMP). The CIRMP's language is less prescriptive than the current licence conditions and would likely fall outside the NSW Government's risk



appetite. Therefore, CyberCX recommends that most of the current licence conditions be retained as they are.

- ▶ The two licence conditions that are recommended for removal relate to the security of personal data. CyberCX recommends that IPART defer to the Privacy Act and CIRMP to regulate the security of personal data within the NSW electricity sector. This is because CyberCX believes that personal data security is of lesser importance to IPART than electricity availability and the OAIC's regulatory powers are within IPART's risk appetite.
- ▶ Some (2/6) of the Compliance licence conditions could be amended, however, they should be amended to reduce the scope of the reporting to only those issues not covered by the Annual Report required by the SOCI Act Critical Infrastructure Risk Management Plan.
 - ▶ The remaining 4/6 Compliance licence conditions should be retained as they are.

DRAFT

2 Context and Background

2.1 Background

IPART has engaged with CyberCX to review the current IPART licence conditions and provide recommendations.

This report will review licence holder's obligations under both the SOCI Act and the Electricity Supply Act 1995, as well as any other regulatory requirements that may relate to licence conditions requirements (eg Privacy Act) This report will then provide IPART with recommendations on the licence conditions in the context of the security landscape of the network operators and the broader regulatory framework to improve regulatory outcomes and minimise any regulatory burden where appropriate.

CyberCX

CyberCX is Australia's largest pure-play cyber security consultancy.

CyberCX is well positioned to assist IPART in this review having gained a wealth of experience in helping government and critical infrastructure asset clients in various aspects of the SOCI Act and other regulatory compliance work including, but not limited to:

- Designing and supporting the implementation of the enhanced cyber security obligations under the reformed SOCI Act.
- Advising on and administering the Hosting Certification Framework on behalf of the Digital Transformation Agency to certify data centres and cloud service providers.
- Supporting industry partners in the energy, utilities and logistics sectors to conform to the SOCI Act through the development and implementation of enterprise cyber security strategies and programs, including data security and supply chain programs.
- Advising foreign-invested companies in their FIRB applications on satisfying SOCI and IPART compliance requirements.
- Advising NSW IPART licence holders on other aspects of their technical cyber security.
- CyberCX's Chief Strategy Officer is a former Head of the Australian Cyber Security Centre, advisor to the Prime Minister, and eSafety Commissioner.

This combination of policy understanding and experience in the practical implications of its implementation places CyberCX as a unique and valuable partner for IPART.

2.2 Document Scope

This report details the approach used to conduct this analysis and summarises both findings and recommendations for uplift to licensing conditions.

The key documents used for analysis as part of this engagement are detailed below.

- ▷ IPART Licensing Conditions.
- ▷ IPART Licensing Principles.
- ▷ Security of Critical Infrastructure Act 2018.
- ▷ Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.
- ▷ Electricity Supply Act 1995.
- ▷ *Privacy Act 1988.*

While not referenced in this report, CyberCX considered the following documents in preparing this report:

- ▶ *AusCheck Act 2007(Cwlth)*.
- ▶ *AusCheck Regulations 2017(Cwlth)*.
- ▶ Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021.
- ▶ Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022.
- ▶ The Instrument of Variation of Conditions of Distributor's Licence released in 2024 (the third instrument of variation).
- ▶ Cyber security framework: Australian Standard AS ISO/IEC 27001:2015.
- ▶ Cyber security framework: Essential Eight Maturity Model published by the Australian Signals Directorate.
- ▶ Cyber security framework: Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States of America.
- ▶ Cyber security framework: Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America.
- ▶ Cyber security framework: The 2020-21 AESCSF Framework Core published by Australian Energy Market Operator.
- ▶ The National Electricity Rules, empowered by the National Electricity Law within *National Electricity (South Australia) Act 1996*.

2.3 Not Legal Advice

Nothing in this deliverable is intended to be taken as legal advice. In preparing this report we have relied upon the information IPART has provided to CyberCX about the laws, codes, regulations, and other obligations that NSW electricity network operators are required to comply with. CyberCX makes no comment as to the appropriateness, applicability, or enforceability of such regulations.

2.4 Threat Landscape

IPART's licence conditions seek to secure NSW electricity infrastructure against cyber attacks that may threaten the availability of electricity. The licence conditions should therefore consider the current and projected threat landscape for NSW electricity infrastructure.

NSW's electricity infrastructure is operating in a dangerous and deteriorating threat environment. IPART should therefore be concerned about ensuring the security of electricity assets through the use of appropriate and risk-informed licence conditions.


Electricity infrastructure has been targeted by nation-state actors

In 2015 and 2016, cyber operatives of Russian military intelligence (GRU) undertook cyber attacks against the Ukrainian power grid.

The December 2015 attack left approximately 230,000 Ukrainians without power for between one and six hours in the middle of winter. The GRU operatives were reportedly able to take 30 substations offline and the backup power for two of three distribution centres.

The December 2016 cyber attack targeted Ukraine's capital city's (Kyiv) electricity infrastructure. The 2016 attack, while smaller in scale, utilised more advanced, automated malware that researchers have suggested could also cause physical damage to the electricity infrastructure.

Importantly for IPART, the Russian Security Services utilised legitimate remote access capabilities to undertake the attacks on Ukrainian infrastructure. Therefore, IPART should have



low risk tolerance for changes to the intended security controls (such as licence conditions 1.1 and 1.2) that would reduce the risk of this known threat vector.

Physical damage to electricity infrastructure has been demonstrated by researchers since 2007, with the first demonstration including the destruction of a 27-ton diesel generator using a cyber attack.

Notably, Australian electricity infrastructure has already been the victim of a cyber attack that has threatened the availability of electricity. In 2021 CS Energy experienced a ransomware attack that threatened the operations of the Callide and Kogan Creek power stations, which provide electricity to 3 million Queenslanders.

Australia should be concerned about the ability and willingness of attackers to disable or destroy electricity infrastructure using cyber attacks.

Australia is vulnerable to cyber attacks

Australia is particularly vulnerable to cyber attacks due to our reliance on digital technology and high rate of digitisation.

Australia's electricity infrastructure is becoming more digitised and remotely accessible. This allows faster and more efficient maintenance, and the ability to leverage expertise from around the world. However, increasingly digitised electricity infrastructure may be more susceptible to cyber attacks than older, less computerised electricity infrastructure.

For example, increasing use of remote access technology has also allowed attackers to access and operate on victim computers. The 2015 attack on the Ukrainian power grid reportedly leveraged remote access technology to gain access to the electricity systems and disable them.

IPART should, therefore, be hesitant to reduce licence conditions design to reduce the risk associated with remote access to licence holder networks.

Worryingly, Australian electricity operators have not tested their ability to undertake a black start while under sustained cyber attack for an advanced adversary.

This is important because the Russian operators targeting Ukraine's electricity grid in 2015 and 2016 targeted the backup and restoration systems to maximise the effect of their attack and impeded operators restoring power.


Any significant cyber attack against Australia's electricity infrastructure by a nation-state actor would likely include attacks aimed to cripple any backup and restoration activities.

As the 2021 CS Energy attack demonstrates, Australia's electricity infrastructure is vulnerable to cyber attacks. This should be mitigated through appropriate and proportionate licence conditions that seek to mitigate the specific threat vectors and types of attacks that have been identified.

The Australian electricity sector is relatively mature compared to other sectors

The Australian electricity sector has a history of being regulated as critical infrastructure. This, and other factors has resulted in the electricity sector having relatively higher security maturity when compared to most Australian industry sectors, including some of the newly defined critical infrastructure sectors.

However, while the electricity sector is generally able to effectively defend against and respond to commodity-level and unsophisticated cyber attacks, the electricity sector should be concerned about state-sponsored cyber attacks. Concerted state-sponsored cyber attacks would likely overwhelm the defences of most Australian electricity providers.



Because of the significant impact of a successful cyber attack on an IPART licence holder, and the ability of sophisticated attackers to overcome most cyber defences; IPART should be comfortable retaining existing licence conditions if there is not another regulatory requirement that produces a similar security outcome commensurate with IPART's risk appetite.

2.5 IPART's Recommended Risk Tolerance

As discussed, electricity is one of Australia's most important critical infrastructures. IPART and the NSW Government should therefore have a low appetite for risks that may threaten the availability of electricity.

CyberCX believes that the availability of electricity is the most important function of licence holders and the most important outcome of licence conditions. This outcome is supported by the various other licence requirements related to the reliability, performance and operation of electricity infrastructure.

While IPART shares this broad responsibility with the Department of Home Affairs, IPART has the specific and sole responsibility to ensure electricity availability within NSW. IPART should therefore have a low appetite for risks that may threaten the availability of electricity.

IPART licence holders also deal with large amounts of personal data. While the confidentiality of data is of concern to IPART and the NSW government, CyberCX believes that it should be of lesser importance than the availability of electricity.

Further, the federal government's Office of the Australian Privacy Commissioner (OAIC) is the responsible regulator and well-placed to enforce the requirements of the *Privacy Act 1988 (Cwlth)*. Because there is an established federal regulator able to enforce regulatory requirements regarding the confidentiality of personal data, and because CyberCX believes the confidentiality of personal data to be of lesser importance than the availability of electricity, CyberCX believes that IPART should have a moderate appetite for risks related to the confidentiality of personal data. IPART should therefore, where reasonable and within risk appetite, defer to the Privacy Act and OAIC on matters related to the confidentiality of personal information held by IPART licence holders.

Due to a history of security regulations and requirements, the NSW electricity sector generally has high cyber security maturity compared to other sectors of the economy. IPART should focus regulatory powers on ensuring compliance with risk-informed licence conditions that are formulated in response to realistic and current threats to ensure the ongoing availability of electricity.

3 Intended Outcomes

3.1 What are critical infrastructure regulations trying to achieve?

Australia's society and economy rely on the continuous provision of critical infrastructure services, including electricity. Australian Commonwealth and State governments have taken on some responsibility to ensure the security and operation of these critical infrastructure assets through the imposition of laws, codes, regulations, and other obligations.

The Commonwealth government outlined its intentions for critical infrastructure security in its 2023 Critical Infrastructure Resilience Strategy (the Strategy). The Strategy describes its purpose as to "anticipate, prevent, prepare for, respond to and recover from all-hazards".⁴

The electricity sector is one of Australia's most critical infrastructure sectors, not only because of its immediate effects but also because of the reliance of other critical infrastructure sectors such as water and telecommunications on electricity. Because of this criticality, it is CyberCX's position that the intention of Australian government regulations should be to ensure the high availability electricity services with the minimum necessary regulatory impost.

The NSW and Australian governments should be primarily concerned with the availability of critical electricity infrastructure that enables the uninterrupted provision of electricity. While data confidentiality is in both government's interests, CyberCX believes that data confidentiality should be a lesser concern that is predominately addressed through the Privacy Act and some SOCI Act requirements.

In regulating critical infrastructure, the main regulatory instrument for the Commonwealth government is the SOCI Act, and the main NSW government regulatory instrument is the licence conditions for the distribution and transmission of electricity in NSW. These licence conditions are administered by IPART on behalf of the Minister for Energy.

3.2 Intended outcomes of the SOCI Act and CIRMP Rules


The Australian 2023 Critical Infrastructure Resilience Strategy describes the intention of the SOCI Act as to "Improve the preparedness of critical infrastructure entities to manage and mitigate the range of hazards that could otherwise have a serious impact on the delivery of their essential service."⁴

The SOCI Act was developed to ensure that entities responsible for critical infrastructure assets "management, preparedness, prevention and resilience business as usual" and "improve information exchange between industry and government".⁵

Notably, as part of the SOCI Act, responsible entities must develop a Critical Infrastructure Risk Management Plan (CIRMP), with the aim to, so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring.

The obligations set out by the SOCI Act in the Critical Infrastructure Risk Management Program give specific consideration to:

- ▶ Personnel security.
- ▶ Supply-chain security.
- ▶ Information security.
- ▶ Natural and physical hazards.



The intended outcome of SOCI Act and supporting artefacts, according to the responsible Minister, is “ensuring the ongoing security and resilience of these [critical infrastructure] assets and the essential services they deliver”.⁶

This report draws heavily on the SOCI Act itself and the legislative instrument which defines the Critical Infrastructure Risk Management Program requirements. Known within the industry as ‘Rule 6’ these requirements are defined in the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, particularly in section 6 of the LIN.

3.3 Intended outcomes of Electricity Supply Act Licence Conditions

The NSW Minister for Energy issues licences for the distribution and transmission of electricity in NSW. These licences are empowered under Schedule 2, section 6 of the Electricity Supply Act 1995.

Schedule 2, section 6(5) of the Energy Supply Act requires the Minister to impose licence conditions related to:

- ▶ Conditions that impose specified performance standards for the reliability of operation of a transmission system and provide for reliability performance monitoring and reporting.
- ▶ Conditions for ensuring that a network operator has arrangements in place to identify, assess and manage business continuity risks and manage business disruptions.
- ▶ Conditions for ensuring that a network operator maintains a substantial operational presence in Australia.

For the purpose of this report, the conditions that will be reviewed here are:


- ▶ Substantial presence in Australia (Condition 1): ensuring substantial Australian control of electricity infrastructure.
- ▶ Data Security (Condition 2): protecting the personal data of Australians, and sensitive data related to the operation of our electricity infrastructure assets.
- ▶ Compliance: ensuring compliance with Conditions 1 and 2 through annual reporting and attestation.

1. Current Substantial Presence in Australia Conditions

The Substantial Presence in Australia licence conditions are intended to ensure that the critical assets and supporting infrastructure are physically located within Australia and not connected to infrastructure or networks that would enable access from outside of Australia. The clauses require that all access, control, management and maintenance related to the asset and supporting infrastructure is conducted by persons located within Australia.

In addition, it aims to ensure a substantial level of Australian control of electricity infrastructure, requiring a minimum of two directors with Australian citizenship, and senior officers with appropriate Australia Government Security Vetting Agency (AGSVA) clearance are appointed to key roles in the management and support of the critical asset.

2. Current Data Security Conditions



The Data Security clauses contained with the licence conditions are intended to ensure that data pertaining to the critical infrastructure and personal data is held in a secure manner; in achieving this, the following themes have been considered:

- ▷ Data may only be stored and accessed from within Australia.
- ▷ Data access is limited to authorised persons.
- ▷ Personal data is held in compliance with the Australian Privacy Act 1988.

3. Current Compliance Conditions

The Compliance clauses within the licence conditions require the licence holder to provide periodic reports to the Tribunal detailing compliance with the Substantial Presence in Australia and Data Security conditions.

IPART uses the following principles for reviewing current licence conditions, and/or to develop new licence conditions:

- ▷ Consumer and community outcomes focused.
- ▷ Proportionate and risk based.
- ▷ Facilitate efficient monitoring and enforcement of compliance.
- ▷ Avoid duplication where possible.
- ▷ Facilitate efficient licence conditions by licence holders.
- ▷ Promote safe, efficient, environmentally responsible and reliable electricity networks.

DRAFT

4 Findings

With the outcomes in mind, CyberCX has compared the two key documents, the SOCI Act and the licence conditions, and developed preliminary findings based on their overlapping conditions. Where Licence conditions have not been referenced, no overlap has been identified and therefore no changes are required.

CyberCX has only recommended that licence conditions be amended or removed if it would not have a detrimental effect on the intended security outcomes of the IPART licence holders. Whilst regulatory duplication is undesirable, the risk of a significant cyber security incident affecting an IPART licence holder is much greater. Therefore, the final state of all changes to licence conditions have been assessed by CyberCX as being with IPART's risk appetite.

4.1 Regulatory Interplay

The SOCI Act and licence conditions have overlapping intended outcomes, that is, securing Australia's critical infrastructure. Notably, the SOCI Act implies a set of requirements on all critical infrastructure entities through the Critical Infrastructure Risk Management Program (CIRMP).

The requirements of the CIRMP overlap with the existing IPART license conditions. This provides an opportunity to streamline IPART license conditions, in alignment with the licence condition principle of 'avoid duplication where possible' and section 30AH(6)(a) of the SOCI Act which indicates that, when formulating the CIRMP rules, the Minister for Home Affairs must have regard to "any existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities"

For this reason, IPART have chosen to review the current licence conditions, assess them against the SOCI Act requirements and other regulatory requirements on licence holders; and update those licence conditions where appropriate.


4.2 Regulatory Authority over the Security of NSW Electricity Assets

Significant proposed changes to the Electricity Supply Act licence conditions would impact on which regulator had primacy over setting security standards for NSW electricity operators.

Currently, the IPART conditions tend to be more prescriptive than the SOCI Act and CIRMP requirements, and so have primacy. This report found that a small number of the 13 Data Security licence conditions could be removed with the outcomes of those licence conditions achieved by SOCI Act and CIRMP requirements. While all 13 of the Data Security licence conditions are related to security outcomes intended by the CIRMP requirements, the licence conditions are more prescriptive and better reflect the risk appetite of IPART and the NSW government.

The NSW Government, through IPART, also assures its own, independent understanding of the security of NSW's electricity infrastructure. Significant changes to the licence conditions would create security outcomes where the NSW Government must rely on information from the federal government to inform its decision making.

However, IPART, on behalf of the NSW Government, would need to be comfortable handing over some responsibility for security requirements setting for NSW electricity operators to the federal Department of Home Affairs.



When making this decision, IPART should consider that the CIRMP rules are defined by legislative instrument and therefore, like the licence conditions, are able to be amended fairly easily. IPART and the NSW government should consider how they would respond to changes to the CIRMP rules to impose greater or lesser security requirements.

Currently, IPART is a mature regulatory entity with established compliance functions and regulatory processes. Home Affairs has only recently begun regulating critical infrastructure security at a large scale and is a maturing capability. IPART and the NSW Government would need to be comfortable giving primary authority to Home Affairs, understanding that it is a less mature regulatory body.

While Home Affairs is the regulator with subject matter expertise in cyber security, IPART has been able to supplement its expertise by engaging with CyberCX. IPART should therefore be comfortable continuing to set licence conditions related to cyber security requirements.

IPART may choose to transfer some regulatory responsibilities to Home Affairs where there is regulatory duplication, and these changes align with IPART's risk appetite. IPART would be able to rely on the Minister's licence-condition-setting power under Schedule 2, section 6 of the Electricity Supply Act to update licence conditions in response to changes to other regulations (such as the CIRMP) or to the cyber threat landscape. However, if licence condition changes were made that deferred certain security outcomes to Home Affairs, it may be difficult for IPART to re-impose more stringent security requirements. This is because increased security requirements would likely invoke a politically sensitive public discussion around the cost increase for end users due to the increased regulatory burden.


4.3 Possible Impact on Regulatory Compliance

IPART and the NSW Government should consider whether the Department of Home Affairs is likely to ensure compliance with the intended security outcomes of the CIRMP requirements as rigorously as IPART currently polices compliance with the licence conditions.

Given the scale of the SOCI Act reforms and the number of responsible entities Home Affairs is now responsible for regulating, it is likely that Home Affairs would not have sufficient resourcing to continue the same level of scrutiny of the four current NSW electricity operators as IPART currently does.

The NSW electricity sector has high cyber security maturity compared to other sectors regulated by the SOCI Act. Given that Home Affairs is responsible for uplifting industry sectors that are less mature than the electricity sector, focus and scarce resourcing may be dedicated to those sectors, to the detriment of enforcing requirements on more mature sectors like the electricity sector. Compared to IPART, Home Affairs, as a new regulator has developing and untested enforcement powers under the SOCI Act, compared to the stronger licence condition powers IPART currently has. Similar cases of enforcing cyber security regulations (such as OAIC v Medibank 2024⁷ and ASIC v RI Advice 2022⁸) have needed to be tested in the courts. There is therefore the potential for initial enforcement actions under the SOCI Act to be tested in the courts, thereby delaying effective enforcement action.

Home Affairs is currently regulating a significant number of responsible entities under the SOCI Act. This would likely stretch Home Affairs's resources and reduce the scrutiny available for each responsible entity. For example, IPART's current licence conditions require that annual attestations of compliance be audited by a third party, the SOCI Act does not require this. If IPART was to reduce licence condition requirements and rely on the SOCI Act requirements, there may be less consistent enforcement action. Given the significance of the electricity sector, IPART should be concerned about any risk to compliance with the intended security outcomes of current licence conditions and the SOCI Act.



IPART and the NSW Government would therefore have less enforcement power for regulating the security of NSW's electricity operators.

4.4 Reduced Security Requirements in some areas

The SOCI Act and CIRMP requirements are generally principle or outcome-based, whereas the IPART licence conditions tend to be more prescriptive in the security controls required.

This is reflective of the broad applicability of the SOCI Act requirements compared to the very niche applicability of the IPART licence conditions.

A significant number of the Significant Presence in Australia and Data Security licence conditions were found to overlap with the CIRMP requirements in section 30AH of the SOCI Act and section 6 of LIN 23/006 (Rule 6).

Section 30AH of the SOCI Act is less stringent than IPART's licence conditions. Section 30AH requires responsible entities to reduce material risk "so far as it is reasonably practicable to do so - minimise or eliminate any material risk of such a hazard occurring".⁹ This is a less stringent requirement than the licence conditions that mandate a security control implementation.

For example, licence condition 2.1b requires that "all load data and bulk personal data records relating to or obtained in connection with the operation of the distribution or transmission system by a Relevant Person is held solely within Australia, and is accessible only by a Relevant Person or a person who has been authorised by the Licence Holder".¹⁰ The SOCI Act s30AH(1)(b)(ii) only requires that the responsible entity "so far as it is reasonably practicable to do so - minimise or eliminate any material risk of the storage, transmission or processing of sensitive operational information outside Australia".⁹

The SOCI Act requirement is therefore less stringent than the current IPART licence condition. IPART and the NSW Government should consider whether the corresponding SOCI Act requirements are commensurate with the government's risk appetite.

CyberCX suggests that IPART's risk appetite should prioritise the availability of electricity. IPART should rely on the CIRMP and Privacy Act to regulate the confidentiality of personal data, specifically load data and bulk personal data. That is because the loss of personal data, while regrettable, is of lesser importance than the loss of availability of electricity to customers. Furthermore, the confidentiality of personal data is already clearly regulated by the OAIC with increased requirements for data security implemented by Home Affairs via the CIRMP.


CyberCX recommends that the NSW government defer to the Privacy Act (and to a lesser extent SOCI Act) to regulate personal data collection and use in the NSW electricity sector.

However, IPART should retain significant security requirements for licence holder's operational technology and associated IT infrastructure as these requirements support the availability of electricity.

4.5 IPART Could Maintain Most Licence Conditions

While IPART could defer a significant number of licence conditions security outcomes to the SOCI Act requirements, IPART should consider keeping specific licence conditions in place to ensure achievement of specific security outcomes.

As discussed above, in most cases the SOCI Act requirements sufficiently align with the intended security outcomes of the licence conditions. However, as the SOCI Act requirements are generally less stringent, IPART should consider implementing licence conditions that specify the way NSW electricity providers must comply with the intended outcomes of their



SOCI Act requirements. This would ensure that licence holders operate within IPART's risk appetite.

For example, licence condition 2.1a currently requires that "The licence holder must ensure that all of its information (being design specifications, operating manuals and the like) as to the operational technology (such as the SCADA system) and associated ICT infrastructure of the operational network is held solely within Australia, and that such information is accessible only by a Relevant Person who has been authorised by the Licence Holder and only from within Australia".

The SOCI Act s30AH(1)(b)(ii) only requires that the responsible entity "so far as it is reasonably practicable to do so - minimise or eliminate any material risk of the storage, transmission or processing of sensitive operational information outside Australia".

IPART may decide that the current licence condition places a significant restriction on Supervisory Control and Data Acquisition (SCADA) system operators to leverage the expertise of their overseas technology providers and therefore hinders their ability to provide electricity services most effectively. However, IPART could also believe that the SOCI Act requirements are too lenient for the State's most critical infrastructure.

In this case, IPART should consider amending the licence condition to provide the licence holder with clear direction on how IPART expects a licence holder to minimise or eliminate material risk as required by the SOCI Act. In this way, IPART clearly maintains the SOCI requirement and does not conflict with it; whilst simultaneously adding an increased requirement to bring licence holders into risk tolerance. None of CyberCX's recommendations conflict with any current CIRMP, SOCI Act or other relevant regulatory requirements.

CyberCX has included these recommendations in section 4.7 Amended Conditions of this report.

4.6 Response from the Department of Home Affairs

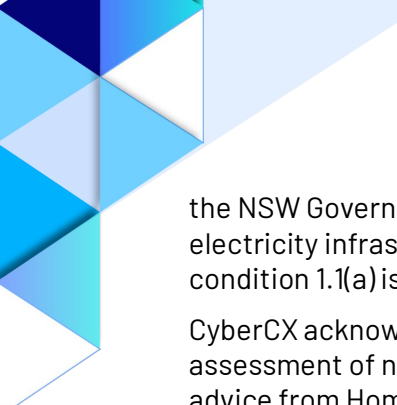
During the process of drafting licence condition changes, The Department of Home Affairs (Home Affairs) was consulted for feedback on the Preliminary Findings version of this report. On 8th September 2024, Home Affairs via the Cyber and Infrastructure Security Centre (CISC) provided additional feedback to IPART.

Given Home Affairs' role as the responsible federal government entity for both cyber security and critical infrastructure policy, CyberCX acknowledges that Home Affairs' comments carry significant weight in any decision regarding cyber security obligations for critical infrastructure entities. CyberCX also acknowledges IPART and Home Affairs share an interest in minimising risks that threaten the availability of electricity.

Most notably in their feedback, Home Affairs recommended that IPART retain licence condition 1.1(a) regarding overseas access to technical environments. Home Affairs views the offshore transmission or access to sensitive data as being very high risk, and considers the steps licence holders should take for their elimination, minimisation and mitigation as key elements of their Critical Infrastructure Risk Management Programs (CIRMP). Home Affairs also conveyed its view that the transmission of sensitive operational information offshore or the provision of remote access should only be done by exception and through a process considered in entities' CIRMPs.

CyberCX recommended that IPART introduce a regime allowing the establishment of physically and logically gapped test environments to allow IPART licence holders to access overseas expertise without allowing access to operational environments.

CyberCX has considered Home Affairs concerns against the initial assessment that overseas access to physically and logically gapped test environments poses a manageable risk and complies with the requirements of the SOCI Act. CyberCX's recommendation sought to balance



the NSW Government's competing requirements for security, and efficient and cost-effective electricity infrastructure. Home Affairs rightly assessed that the current IPART licence condition 1.1(a) is a higher security standard than the SOCI Act requires.

CyberCX acknowledges that Home Affairs is the responsible federal entity and defers to its assessment of national risk. On this basis CyberCX considers it reasonable to prioritise the advice from Home Affairs and retain the current licence condition 1.1(a) as is.

DRAFT

4.7 Overlapping Conditions

During document analysis, CyberCX identified the following **IPART licence conditions that had overlapping outcomes or intentions as the SOCI Act obligations**. These have been grouped based on their licence condition category below.

Please note: LIN 23/006 refers to the legislative instrument 23/006 Security of Critical Infrastructure (Critical infrastructure risk management program) Rules. ¹¹

4.7.1 Overlapping Conditions - Data Security

Section	Licence Condition Summary	Finding	Recommendation
2.1.c	This licence condition states that the entity does not export and has appropriate security controls in place to prevent the export, of Bulk Personal Data Records relating to or obtained in connection with the operation of the distribution or transmission system by a Relevant Person, outside of Australia.	<p>When comparing this licence condition to the SOCI Act, Section 2A states entities "must have, and comply with, a critical infrastructure risk management program", a CIRMP. As per the LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 6 Material Risks 6d, states that entities must address a material risk for the "storage, transmission or processing of sensitive operational information outside Australia, which includes: (vi) data that a reasonable person would consider to be confidential or sensitive about the asset; 6e requires that, entities must address a material risk for "remote access to operational control or operational monitoring systems of the CI asset".</p> <p>Section 8 Cyber and information security hazards 8(2)(a) "minimise or eliminate any material risk of a cyber and information security hazard occurring." 8(2)(b) mitigate the relevant impact of a cyber and information security hazard on the CI asset.</p> <p>CyberCX therefore assess that the security outcome of ensuring the confidentiality of personal data is sufficiently addressed by the relatively mature OAI C enforcement of the Privacy Act in Australian Privacy Principle 8, and section 6(d)(vi) of LIN 23/006. IPART should therefore be comfortable to remove this licence condition whilst remaining within risk appetite.</p>	<p>Consider Removing. While the licence condition outlines more stringent requirements, it is a specific means to mitigate a material risk as per Section 8.</p> <p>Additionally, given the requirements set out in the Privacy Act (1988), particularly Australian Privacy Principles (APP) 8 (cross-border disclosure of personal information) and 11 (security of personal information), licensees should consider Bulk Personal Data Records as sensitive information and treat it with the requirements set out under s6.d of the LIN.</p> <p>This licence condition may be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary and achieve the intended outcome.</p>



Table 3 – Overlapping Conditions - Data Security in Australia

DRAFT

4.8 Amend conditions

During document analysis, CyberCX identified the following **IPART licence conditions that have some relationship to SOCI Act requirements and could be amended to consider the SOCI Act requirements.**

4.8.1 Amend Conditions - Substantial Presence in Australia

Section	Licence Condition Summary	Finding	Recommendation
1.1	Except to the extent allowed for under the Protocol agreed with the Commonwealth Representative, the Licence Holder must take all practical and reasonable steps to ensure:		Consider Amending Condition Amend the current licence condition to: "Except to the extent allowed for under the Protocol agreed with the Commonwealth Representative; the Licence Holder must take all practical and reasonable steps, commensurate with the risk to the licence holder and/or wider electricity network, to ensure:

DRAFT

<p>1.1a</p>	<p>As far as reasonably possible, all maintenance of the responsible entities distributed system must be undertaken solely from within Australia.</p> <p>With exemption to cases where physical servicing of components or acquisition of replacement components is required.</p>	<p>This licence condition is a more specific requirement that achieves the intended outcome of the RMP. When comparing this licence condition to the SOCI Act, Section 2A states entities “must have, and comply with, a critical infrastructure risk management program”, a CIRMP. As per the Legislative Instrument 23/006 (LIN 23/006) the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 10 Supply Chain Hazards Section 10(1)(a) of the LIN requires that SOCI Act responsible entities “minimise or eliminate the following material risks” related to supply chains but only “as far as it is reasonably practicable to do so”. The IPART requirement includes the phrase “as far as reasonably possible”, which produces the same outcome as the CIRMP requirement. This is therefore a duplication that does not provide any increase in security outcomes. IPART should remove the licence condition and rely on the CIRMP requirement.</p> <p>Section 6 Material Risks S6e stipulates that entities must address a material risk for “remote access to operational control or operational monitoring systems of the CI asset”.</p> <p>Section 7 General Hazards Section 7(c)(i) requires that responsible entities “as far as it is reasonably practicable to do so – minimise or eliminate the material risk which may include those mentioned in section 6”.</p> <p>Section 9 Personnel Hazards 1b states that to “permit a critical worker access to critical components of the Critical Infrastructure (CI) asset only where the critical worker has been assessed to be suitable to have such access”. S5b states that “whether permitting a critical worker to have access to critical components of the CI asset would be prejudicial to security”. Finally, 5c states that “any other information that may affect the person’s suitability to have access to the critical components of the CI asset”.</p>	<p>Consider Amending Condition This licence condition outlines the requirements, to mitigate a material risk as per Section 6.</p> <p>This licence condition could be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary. The use of the terms “reasonably possible” and the inclusion of an exemption make this licence condition no stronger than the SOCI Act requirements.</p> <p>However, given that this is an existing requirement, and the NSW government’s risk appetite, CyberCX suggests amending this condition to include scope for overseas servicing of distributed system where that system has been separated from the remainder of the network. CyberCX recommends the licence condition be amended to the following:</p> <p>“As far as reasonably possible, all maintenance of the responsible entities distributed system must be undertaken solely from within Australia.</p> <p>Licence holders may establish a controlled test/maintenance environment, physically segmented from the licence holder’s operational environment. This licence condition requires physical segmentation of the network, logical segmentation such as the use of a virtual local area network (VLAN) would not be compliant. Overseas maintenance or testing of systems /components may occur in the segmented test environment.</p> <p>Any movement of data between the segmented test environment and the licence holder’s operational environment must be directed and controlled from within Australia.</p> <p>With exemption to cases where physical servicing of components or acquisition of replacement components is required.”</p>
-------------	---	--	--

Section	Licence Condition Summary	Finding	Recommendation
1.3b	<p>The licence holder must have senior officers responsible for (not withstanding their title):</p> <ul style="list-style-type: none"> ➤ Operational technology ➤ Network operations ➤ Security operations <p>In relation to its distribution or transmission systems, who are persons residing in Australia and hold an appropriate national security clearance, being a clearance of not less than Negative Vetting Level 1 (or equivalent) issued by the NSW Government on advice from the Australian Government Security Vetting Agency (AGSVA).</p>	<p>CyberCX found no overlap between the condition requiring senior officers responsible for operational technology, network operations, and security operations.</p> <p>However, section 30AH of the SOCI Act allows the CIRMP to include requirements for a background check under the AusCheck scheme for employees of a responsible entity.</p> <p>Section 9(1)(b) of LIN 23/006 requires a responsible entity “to permit a critical worker access to critical components of the CI asset only where the critical worker has been assessed to be suitable to have such access” and s9.1.c.i requires them to minimize or eliminate the risk from “malicious or negligent employees”.</p> <p>The CIRMP requirements therefore achieve the intended outcome of requiring an AGSVA NV1 clearance or higher.</p> <p>As per s9(2) of the LIN, responsible entities may require a background check conducted under the AusCheck scheme for their staff. This requirement directly overlaps with the current licence condition requirement for an NV1 clearance without contributing to a meaningful increase in security.</p>	<p>Consider Amending Condition</p> <p>The current licence condition requires senior officers to hold an AGSVA NV1 security clearance or higher.</p> <p>The intention of this requirement is to ensure that senior officers with responsibility for the operation of critical infrastructure are in good standing and unlikely to be manipulated by bad actors.</p> <p>The SOCI Act CIRMP considers personnel hazards as one of the key risks to critical infrastructure. The requirement for AusCheck background checks, and section 9.1 of LIN 23/006 empower NSW electricity operators to achieve the same intended outcomes as the current licence condition.</p> <p>CyberCX therefore recommends that IPART replace the following section of licence condition 1.3b: “being a clearance of not less than Negative Vetting Level 1 (or equivalent) issued by the NSW Government on advice from the Australian Government Security Vetting Agency (AGSVA).” and replace it with the following: “being an a background check conducted under the AusCheck scheme, conducted as per the Critical Infrastructure Risk Management Program requirements stipulated in section 9 of federal legislative instrument 23/006.”</p> <p>Consider adding a requirement that “licence holders must provide IPART with a copy of the results of the AusCheck background check and their assessment of the suitability of the senior officer to hold that position.”</p>

Section	Licence Condition Summary	Finding	Recommendation
1.5a	The exception in condition 1.4b of Appendix 2 ceases to apply to the licence holder if an appointment and application for national security clearance for the person is not made within 4 months of (as relevant) the first issue of these conditions or the relevant vacancy or disqualification occurring; or	The proposed AusCheck background check is not a "national security clearance" in the same way an AGSVA NV1 clearance is. Propose updating this language to clarify and avoid confusions.	<p>Consider Amending Condition</p> <p>Recommend replacing "national security clearance" with "appropriate security vetting".</p>

DRAFT

Section	Licence Condition Summary	Finding	Recommendation
1.4b	<p>The licence holder is not in breach of its obligations under</p> <p>a) Condition 1.3 of Appendix 2 if following:</p> <ul style="list-style-type: none"> i. the first issue of these conditions to the licence holder; or ii. any position identified in condition 1 being vacated or the relevant person ceasing to satisfy the qualifications set out there for any reason, <p>The licence holder:</p> <ul style="list-style-type: none"> iii. procures the appointment of a person to the relevant position that the licence holder bona fide believes will be able to obtain the required security clearance; and <p>has procured that the person applies for the required security clearance.</p>	<p>The proposed AusCheck background check is not a "national security clearance" in the same way an AGSVA NV1 clearance is. Propose updating this language to clarify and avoid confusions.</p>	<p>Consider Amending Condition</p> <p>Recommend replacing "national security clearance" with "appropriate security vetting".</p>

Table 4 - Amended Conditions - Significant Presence



DRAFT

4.8.2 Amend Conditions - Data Security

Section	Licence Condition Summary	Finding	Recommendation
2.1a	<p>The licence holder must ensure that all of its information including design specifications, operating manuals and the like related to the operational technology (such as the SCADA Systems) and associated ICT infrastructure of the operational network is held solely within Australia.</p> <p>It also requires that such information is only accessible by a Relevant Person who has been authorised by the licence holder and only from within Australia.</p>	<p>When comparing this licence condition to the SOCI Act, Section 2A states entities “must have, and comply with, a critical infrastructure risk management program”, a CIRMP. As per LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 6 Material Risks 6d, states that entities must address a material risk for the “storage, transmission or processing of sensitive operational information outside Australia, which includes:</p> <ul style="list-style-type: none"> (i) layout diagrams; (ii) schematics; (iii) geospatial information; (iv) configuration information; (v) operational constraints or tolerances information; (vi) data that a reasonable person would consider to be confidential or sensitive about the asset; <p>6e, entities must address a material risk for “remote access to operational control or operational monitoring systems of the CI asset”.</p> <p>Section 7 General Hazards 7(c)(i) requires that responsible entities “as far as it is reasonably practicable to do so – minimise or eliminate the material risk which may include those mentioned in section 6”</p> <p>Section 9 Personnel Hazards, 1b states that to “permit a critical worker access to critical components of the Critical Infrastructure (CI) asset only where the critical worker has been assessed to be suitable to have such access” and 5b states that “whether permitting a critical worker to have access to critical components of the CI asset would be prejudicial to security”. Finally, 5c states that “any other information that may affect the person’s suitability to have access to the critical components of the CI asset”.</p>	<p>Consider Amending The SOCI Act requirements compel the entity to mitigate the risk whereas this licence condition prescribes the way the risk should be mitigated.</p> <p>This licence condition may be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary.</p> <p>However, CyberCX recommends that IPART amend the licence condition to stipulate how it expects licence holders to comply with the outcome prescribed in LIN 23/006.</p> <p>IPART should consider implementing a requirement to the effect of the following: “To reduce the risk of mishandling of sensitive information, if a third party requires access to this information and is approved to do so, it must only be accessed in a controlled environment segregated from the operational network as per licence condition 1.1a. Third parties must not be given access to the licence holder’s network to access sensitive documentation.”</p>

Section	Licence Condition Summary	Finding	Recommendation
2.1b	<p>This licence condition states that all load data and bulk personal data records relating to or obtained in connection with the operation of the distribution or transmission system by a Relevant Person is held solely within Australia.</p> <p>It also states these must be accessible only by a Relevant Person or a person who has been authorised by the licence holder.</p>	<p>When comparing this licence condition to the SOCI Act, Section 2A of the SOCI Act states that entities “must have, and comply with, a critical infrastructure risk management program”, a CIRMP. As per the LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 6 Material Risks S6d, states that entities must address a material risk for the “storage, transmission or processing of sensitive operational information outside Australia, which includes: (vi) data that a reasonable person would consider to be confidential or sensitive about the asset; 6e, entities must address a material risk for “remote access to operational control or operational monitoring systems of the CI asset”.</p> <p>Section 7 General Hazards 7c(i) requires that responsible entities “as far as it is reasonably practicable to do so – minimise or eliminate the material risk which may include those mentioned in section 6”.</p>	<p>Consider Amending IPART should consider limiting this licence condition to only load data. To do so would require the removal of the phrase “and bulk personal data records” from the licence condition.</p> <p>Given the requirements set out in the Privacy Act (1988), particularly Australian Privacy Principles (APP) 8 (cross-border disclosure of personal information) and APP 11 (security of personal information), licence holders should consider Bulk Personal Data Records as sensitive information and treat it with the requirements set out under s6(d) of the LIN.</p> <p>Furthermore, CyberCX assesses that IPART’s primary concerns should be to the availability of the licence holder’s systems and the delivery of electricity. Personal data security is therefore of a lower priority. The requirements of the SOCI Act and Privacy Act are therefore commensurate with IPART’s risk appetite.</p> <p>While s6(d)(vi) of the LIN could be taken to include security requirements for load data, due to the NSW government’s risk tolerance, it is recommended that this licence condition be retained for load data.</p> <p>However, IPART should consider continuing this requirement for load data given its operational importance.</p>

Section	Licence Condition Summary	Finding	Recommendation
2.4	<p>The licence holder must ensure that third party data or information (including without limitation communications within the meaning of the Telecommunications (Interception and Access) Act 1979 (Cth), personal information within the meaning of the Privacy Act 1988 (Cth), and closed-circuit television footage) which is indirectly accessed or obtained by the licence holder because that third party data or information is transferred by a carrier or other party using the licence holders infrastructure, are held by the licence holder solely within Australia, and are accessible only by a Relevant Person or a person who has been authorised by the licence holder and, in each case, only from within Australia.</p>	<p>When comparing this licence condition to the SOCI Act, Section 2A states entities “must have, and comply with, a critical infrastructure risk management program”, a CIRMP. As per the LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 6 Material Risks 6d, states that entities must address a material risk for the “storage, transmission or processing of sensitive operational information outside Australia, which includes: (vi) data that a reasonable person would consider to be confidential or sensitive about the asset; 6e, entities must address a material risk for “remote access to operational control or operational monitoring systems of the CI asset”.</p> <p>Section 9 Personnel Hazards, 1b states that to “permit a critical worker access to critical components of the Critical Infrastructure (CI) asset only where the critical worker has been assessed to be suitable to have such access” and 5b states that “whether permitting a critical worker to have access to critical components of the CI asset would be prejudicial to security”. Finally, 5c states that “any other information that may affect the person’s suitability to have access to the critical components of the CI asset”.</p>	<p>Consider Amending While the licence condition outlines more stringent requirements, it is a specific means to mitigate a material operational risk as per Sections 6 and 9.</p> <p>This licence condition may be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary and achieve the intended outcome.</p> <p>However, CyberCX recommends that IPART amend the licence condition to stipulate how it expects licence holders to comply with the outcome prescribed in LIN 23/006.</p> <p>IPART should consider implementing a requirement to the effect of the following: “To reduce the risk of mishandling of sensitive information, if a third party requires access to this information and is approved to do so, it must only be accessed in a controlled environment segregated from the operational network as per licence condition 1.1a. Third parties must not be given access to the licence holder’s network to access sensitive documentation.”</p>

Table 5 - Amend Conditions - Data Security

4.8.3 Amend Conditions - Compliance

Section	Licence Condition Summary	Finding	Recommendation
3.1	This licence condition states that by 30 September each year, the licence holder must produce a report detailing whether the licence holder has complied with the conditions set out over the preceding financial year."	There is a duplication of effort between the SOCI Act and this licence condition. The SOCI Act requires responsible entities to provide an annual CIRMP report.	<p>Consider Amending Condition</p> <p>The current intention of the Compliance licence conditions is to ensure compliance with Conditions 1 and 2. Given significant recommended changes to Conditions 1 and 2, it is recommended that the licence holder provide IPART with a copy of the Annual CIRMP Report required under s30AG of the SOCI Act, and that a much smaller report be provided by the Licensee for remaining conditions that are not covered by the SOCI Act.</p> <p>CyberCX recommends that compliance license condition s3.1 be amended to have a similar effect to the following:</p> <p>"By 30 September each year the licence holder must furnish a report to the Tribunal and the Commonwealth Representative two reports. The first is the Annual Report required under section 30AG of the Security of Critical Infrastructure Act 2018.</p> <p>The second report should detail, to the extent that it is not covered by the Annual Report, whether the licence holder has complied with conditions 1 and 2 of Appendix 2 over the preceding financial year to 30 June."</p>
3.4	The report required under condition 3.1 of this Appendix 2 must be accompanied by a certification in writing supported by a resolution of the Board of the licence holder that, with respect to the relevant period:	This licence condition is commensurate with s30AG(2)(f) of the SOCI Act which requires attestation of the CIRMP Annual Report by the Board or other Governing Body.	<p>Consider Amending Condition</p> <p>Given significant changes to Conditions 1 and 2, it is recommended that the licence holder provide IPART with a copy of the Annual CIRMP Report required under s30AG of the SOCI Act, and that a much smaller report be provided by the Licensee for remaining conditions that are not covered by the SOCI Act. This report should be approved by the Board or Governing Body.</p>

Table 6 - Amended Conditions - Compliance

4.9 Retained Conditions

During document analysis, CyberCX identified the following **IPART licence conditions that had no overlapping or conflicting conditions in IPART's licence conditions against the SOCI Obligations**. These licence conditions are not affected by the SOCI Act requirements and should remain as they are. These licence conditions have been grouped based on their category below.

4.9.1 Independent Conditions - Substantial Presence in Australia

Section	Licence Condition Summary	Finding	Recommendation
1.1b	Any third-party or non-licence holder employee from outside Australia, undertaking maintenance of the distributed system is subject to approval of the senior officer responsible for network operations.	<p>When comparing this licence condition to the SOCI Act, Section 2A states entities "must have, and comply with, a critical infrastructure risk management program", a CIRMP. As per LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 6 Material Risks 6e, entities must address a material risk for "remote access to operational control or operational monitoring systems of the CI asset".</p> <p>Section 7 General Hazards Section 7(c)(i) requires that responsible entities "as far as it is reasonably practicable to do so - minimise or eliminate the material risk which may include those mentioned in section 6"</p> <p>Section 9 Personnel Hazards, 1b states that to "permit a critical worker access to critical components of the Critical Infrastructure (CI) asset only where the critical worker has been assessed to be suitable to have such access" and 5b states that "whether permitting a critical worker to have access to critical components of the CI asset would be prejudicial to security". Finally, 5c states that "any other information that may affect the person's suitability to have access to the critical components of the CI asset"</p>	<p>No Change Required. While the licence condition outlines more stringent requirements, it is a specific means to mitigate a material risk as per Section 6 of the LIN.</p> <p>This licence condition could be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary.</p> <p>However, given IPART's risk appetite and the threat to system availability that is created through remote access, CyberCX recommends that IPART retain this licence condition.</p>

Section	Licence Condition Summary	Finding	Recommendation
1.2a	<p>The distributed system must only be accessible, operated, and controlled from within Australia or be connected to any other distributed system or infrastructure that could enable access, operation or control.</p>	<p>The CIRMP requirements under s8 and s6(e) of LIN 23/006 attempts to achieve a similar outcome to this licence condition.</p> <p>However, this licence condition is more prescriptive and stringent than the SOCI Act requirements.</p> <p>Given IPART's risk appetite for malicious access and control of licence holder systems, it is recommended that this licence condition be retained as is.</p>	<p>No Change Required</p> <p>While the licence condition outlines more stringent requirements, it is a specific means to mitigate a material risk as per Section 6.</p> <p>This licence condition may be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary.</p> <p>However, due to the significant risk to the availability of licence holder systems posed by unauthorized remote access, CyberCX recommends that the licence condition be retained as is. It is unlikely that the SOCI Act requirement sufficiently addresses the risk, commensurate with IPART's risk appetite.</p>

DRAFT

Section	Licence Condition Summary	Finding	Recommendation
1.2b	The licence holder must notify the regulator in advance of any engagement with the market to outsource the operation or control of its distributed system.	<p>When comparing this licence condition to the SOCI Act, Section 2A states entities “must have, and comply with, a critical infrastructure risk management program”, a CIRMP. As per the LIN 23/006 the CIRMP must establish and maintain a process or system to address the following requirements:</p> <p>Section 9 Personnel Hazards 9c “as far as it is reasonably practicable to do so—to minimise or eliminate the following material risks: (i) arising from malicious or negligent employees or contractors.</p>	<p>No change required While the licence condition outlines more stringent requirements, it is a specific means to mitigate a material risk as per Section 9 of LIN 23/006.</p> <p>This licence condition may be removed to defer to the SOCI Act CIRMP requirements to allow responsible entities to mitigate risk as they deem necessary.</p> <p>However, given the risk to electricity availability of outsourcing of the operation or control of critical electricity assets, CyberCX recommends that this risk continue to be managed by a directly relevant licence condition.</p>
1.3a	The licence holder must have at least two directors who are Australian citizens.	<p>CyberCX found no overlapping or conflicting conditions in this licence condition against the SOCI Obligations.</p> <p>This is a reasonable requirement for critical infrastructure providers. IPART may consider whether a proportion or percentage-based requirement (e.g >50% of directors) would be better suited to achieving the intended security outcome.</p> <p>There may be some overlap here with Foreign Investment Review Board (FIRB) requirements, however this is a more stringent requirement that is commensurate with IPART’s risk appetite.</p>	<p>No Change Required Maintain this licence condition.</p>

Section	Licence Condition Summary	Finding	Recommendation
1.4a	The licence holder is not in breach of its obligations under b) Condition 1.3a of Appendix 2 if, in the case of a casual vacancy on the board of directors, the vacancy is filled within two months of the casual vacancy first occurring; and	CyberCX found no overlapping or conflicting conditions in this licence condition against the SOCI Obligations.	No Change Required Maintain this licence condition.
1.5b	The exception in condition 1.4b of Appendix 2 ceases to apply to the licence holder if a) If the application referred to in condition 1.5(a) is made and is rejected or withdrawn, the licence holder does not procure a replacement application being made within 4 months of that rejection or withdrawal; or	CyberCX found no overlapping or conflicting conditions in this licence condition against the SOCI Obligations.	No Change Required Maintain this licence condition.
1.5c	The exception in condition 1.4b of Appendix 2 ceases to apply to the licence holder if: b) the licence holder does not procure compliance with condition 1.3(b) in any event with respect to any position within 8 months (or such longer period as approved in writing by the Minister) of (as relevant) the first issue of these conditions or the relevant vacancy occurring.	CyberCX found no overlapping or conflicting conditions in this licence condition against the SOCI Obligations.	No Change Required Maintain this licence condition.

Table 7 - Independent Conditions - Substantial Presence in Australia

4.9.2 Independent Conditions - Data Security

Section	Licence Condition Summary	Finding	Recommendation
2.2	<p>This licence condition states that the licence holder is not in breach of its obligations under conditions 2.1:</p> <p>(a), 2.1(b)(i) or 2.1(c) of this Appendix 2 if the licence holder discloses, holds, uses or accesses any information or data referred to in those conditions, or the licence holder allows a Relevant Person approved by the senior officer referred to in condition 1.3(b)(i) of this Appendix 2 to disclose, hold, use or access any information or data referred to in those conditions for the purposes of:</p> <p>2.2a) Disclosure to a recognised stock exchange so that such information is made available publicly in compliance with a binding obligation on the part of the licence holder or an Associate to do so;</p> <p>2.2b) Complying with any law of the Commonwealth of Australia, or of any of its States and Territories;</p> <p>2.2c) Disclosure to the financial, accounting, insurance, legal, regulatory and other advisers, auditors, insurers, security trustees and financiers (and each of their advisers) of the licence holder, any Associate, and any bona fide prospective purchaser of any interest in, or of any interest in the main undertaking of, the licence holder or any Associate, but in each case only to the extent necessary in order for those persons to provide the advisory or other services bona fide required of them;</p> <p>2.2d) Disclosure to participants, regulators and service providers in the electricity sector, provided it is in the ordinary course of business and in accordance with good electricity industry practice, and such information is required by those persons to provide the services or to perform the functions bona fide required of them;</p> <p>2.2e) Providing aggregated data which does not permit identification of any particular customer or customers connection points or their demand characteristics;</p> <p>2.2f) Allowing a service provider or contractor to hold, use or access information where that arrangement is approved by the Tribunal, in the case of arrangements approved as of the first issue of these conditions, and otherwise where the licence holder has provided the Commonwealth Representative with a submission demonstrating that: (i) the service provider or contractor is reputable; and (ii) the service provider or contractor has data security systems in place to ensure information security is maintained; and has obtained the written agreement of the Commonwealth Representative for the arrangement;</p> <p>2.2g) Such other circumstances as approved by the Tribunal in writing. Prior to seeking approval from the Tribunal, the licence holder must provide the Commonwealth Representative with a reasonable opportunity within a period not ending less than 60 calendar days, to confirm in writing to the Tribunal that the Commonwealth does not intend to make any further requests or submissions in relation to the matter.</p>		<p>No change required</p> <p>The retention of licence conditions 2.1a, b, and c requires the retention of this licence condition.</p>
2.3	<p>The licence holder is not in breach of its obligations under condition 2.1(b)(ii) of this Appendix 2 if a Relevant Person or a person authorised to access the information by the licence holder discloses, holds, uses or accesses personal information in accordance with the Privacy Act 1988 (Cth).</p>		<p>No change required</p> <p>The retention of licence conditions 2.1a, b, and c requires the retention of this licence condition.</p>

Table 3 - Independent Conditions - Data Security

4.9.3 Independent Conditions - Compliance

Section	Licence Condition Summary	Finding	Recommendation
3.3	The Tribunal may provide guidance to the Approved Critical Infrastructure Auditor as to the licence holder's practices that have satisfied or will satisfy conditions 1 and 2 of this Appendix 2.	CyberCX found no overlapping or conflicting conditions in this licence condition against the SOCI Obligations.	No Change Required If IPART chooses to require an annual report from NSW electricity operators (which is recommended) then IPART should maintain this licence condition.
3.2	The report required under condition 3.1 of this Appendix 2 must be audited by an Approved Critical Infrastructure Auditor by a date specified by the Tribunal. The audit required by this condition 3.2 must be a comprehensive audit and must meet any requirements specified by the Tribunal. licence holder must provide the audited report to the Commonwealth Representative at the same time that the report is provided to the Tribunal.	There is no SOCI Act requirement for entities to perform an external audit of the CIRMP report. Therefore, this is an extra requirement from the licence conditions for NSW Electricity network operators.	No Change Required If IPART chooses to require an annual report from NSW electricity operators (which is recommended) then IPART should maintain this licence condition.
3.4a	The licence holder has complied with conditions 1 and 2 of this Appendix 2; or	This licence condition is commensurate with s30AG(2)(c)(i) of the SOCI Act which requires the responsible entity to attest as to whether their CIRMP was "up to date at the end of the financial year".	No Change Required If IPART chooses to require an annual report from NSW electricity operators (which is recommended) then IPART should maintain this licence condition.

Section	Licence Condition Summary	Finding	Recommendation
3.4b	The licence holder has not complied with conditions 1 and 2 of this Appendix 2 and certifying the nature and extent of each non-compliance and the steps taken by the licence holder to ensure compliance (and to preclude further non-compliance) and the timeframe within which it expects to achieve compliance.	This licence condition is commensurate with s30AG(2)(c)(ii) of the SOCI Act which requires the responsible entity to attest as to whether their CIRMP was “not up to date at the end of the financial year”.	No Change Required If IPART chooses to require an annual report from NSW electricity operators (which is recommended) then IPART should maintain this licence condition.

Table 9 - Independent Conditions - Compliance

DRAFT

Appendix A Endnotes

¹ Physical security and natural, cyber and information security, personnel, supply chain.

² Resource Management Guide - Regulator Performance, accessed 11 July, 2024.
<https://www.regulatoryreform.gov.au/regulator-performance>

³ Hosting Certification Framework, accessed 11 July, 2024.
<https://www.hostingcertification.gov.au/>

⁴ CISC (Cyber and Infrastructure Security Centre)(2023), *Critical Infrastructure Resilience Strategy 2023*, Australian Government Department of Home Affairs, accessed 27 June 2024,
<https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf>

⁵ CISC (Cyber and Infrastructure Security Centre)(2023), *Regulatory obligations*, Australian Government Department of Home Affairs, accessed 27 June 2024, <https://www.cisc.gov.au/how-we-support-industry/regulatory-obligations>

⁶ CISC (Cyber and Infrastructure Security Centre)(2023), *Explanatory document SLACIP*, Australian Government Department of Home Affairs, accessed 27 June 2024,
<https://www.homeaffairs.gov.au/reports-and-pubs/files/explanatory-document-SLACIP.pdf>

⁷ *Australian Information Commissioner v Medibank Private Limited ACN 080 890 259 (2024) Office of the Australian Information Commissioner*. Available at:
https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf (Accessed: 11 July 2024).

⁸ *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496 (2022) Australian Securities and Investments Commission*. Available at:
<https://download.asic.gov.au/media/zhodijpp/22-104mr-2022-fca-496.pdf> (Accessed: 11 July 2024).

⁹ Security of Critical Infrastructure Act 2018, No. 29, 2018, Compilation No. 6, Compilation date: 20 October 2023, includes amendments up to Act No. 76, 2023, registered 28 October 2023

¹⁰ IPART (Independent Pricing and Regulatory Tribunal)(2017), *TransGrid operating licence: consolidated licence conditions from November 2017*, accessed 27 June 2024,
<https://www.ipart.nsw.gov.au/sites/default/files/documents/transgrid-operating-licence-consolidated-licence-conditions-from-november-2017.pdf>

¹¹ Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023