IPART Cyber Security Licence Conditions Review

Supplemental Response

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

DATE: 3 April 2025

Lead Author: Lachlan McGrath | Manager – Strategy & Consulting

Key Details

Project Details

Client Details	
Client Name	IPART
Client Contact	Christine Allen

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 4

2 Context and Background 5

2.1 Background 5
2.2 Not Legal Advice 6
3 Findings 7

3.1 Definition of 'Components' 7
3.2 Definition of 'Physical Servicing' 7
3.3 Providing IPART with a copy of the SOCI Act Annual Report 8
3.4 Definition of 'ICT Infrastructure' 9
3.5 Definition of 'Operational Technology' 9
3.6 Definitions of 'Third Party Data' and 'Sensitive Information' 10

Tables

Table 1 - Project Details 2
Table 2 - CyberCX Contact Details 2

1 Executive Summary

On 15th November 2024, the New South Wales (NSW) Independent Prudential and Regulatory Tribunal (IPART) released a set of documents as part of its review into of electricity network operators' critical infrastructure licence conditions. These documents included:

- A Draft Report from IPART.
- A Draft Report from CyberCX.
- Draft Critical Infrastructure Licence Conditions.

IPART requested public consultation on the draft licence conditions to be submitted by Friday 20 December 2024. All four licence holders provided written comments to IPART.

IPART has reviewed the licence holder's comments and requested CyberCX to respond to particular comments therein. This deliverable outlines CyberCX's response to IPART where that response has been sought.

This Supplemental Response document should be read and understood in conjunction with CyberCX's original report to IPART. At the time of writing, this original report is available on IPART's website as part of the public consultation on the review of electricity network operators' critical infrastructure licence conditions.

2 Context and Background

2.1 Background

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 domains 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 Guide, 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.

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 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.

3 Findings

3.1 Definition of 'Components'

Licence Condition

Licence condition 2.2 reads:

"Despite condition 2.1., the Licence Holder may acquire components from outside Australia and conduct physical servicing of components outside Australia for the purposes of maintenance of the System where:

a) it is not reasonably practicable to acquire the components or conduct physical servicing from within Australia, and
b) the senior officer with Network Operations Responsibility approves the acquisition from, or physical servicing by, a specific person or Entity."

Response from Licence Holders

Licence holders have raised the concern that 'components' does not currently have an explicit definition in the licence conditions. Licence holders have suggested that 'Components' in this context should be defined to not include maintenance of primary assets that do not contain active equipment (e.g. electronic processor capabilities or communications capability) such as poles, pole hardware (e.g. fittings and fixtures), conductors and serviceable parts of primary assets, such as circuit breaker contacts and mechanisms.

CyberCX's Response

"CyberCX recommends that IPART define 'components' to have a similar meaning to the following:

'Components refers to any part of the system that contains electronic processor capabilities, electronic storage of data or communications capability. Where an asset contains serviceable parts in addition to a component as described the entire asset is considered a component unless these parts are removed.'

3.2 Definition of 'Physical Servicing'

Licence Condition

Licence condition 2.2 reads:

"Despite condition 2.1, the Licence Holder may acquire components from outside Australia and conduct physical servicing of components outside Australia for the purposes of maintenance of the System where:

a) it is not reasonably practicable to acquire the components or conduct physical servicing from within Australia, and
b) the senior officer with Network Operations Responsibility approves the acquisition from, or physical servicing by, a specific person or Entity."

Response from Licence Holders

Licence holders have raised the concern that the term 'physical servicing' used in section 2.2 is not explicitly defined. Licence holders have indicated that they believe that it refers to components that are taken off the system, serviced, and returned onto the system.

In their feedback, licence holders have requested that IPART consider whether physical servicing should be defined to exclude virtual servicing from outside of Australia, and to consider whether software debugging, patches, new version components etc can, or cannot, be undertaken from outside of Australia.

CyberCX's Response

Due to the requirements of licence condition 2.3, non-physical servicing cannot occur from outside Australia without an agreement with the Department of Home Affairs.

If IPART chose to define physical servicing, it could consider words to the effect of:

'The inspection or adjustment of components from live systems or inventory for the purpose of maintenance or upgrade, including the removal and reinstallation of components for inspection or adjustment in third party locations.'

A reading of the current licence conditions suggests that debugging could occur on an image of the system from outside Australia. However, overseas access to the system itself is not allowed under licence condition 2.3.

3.3 Providing IPART with a copy of the SOCI Act Annual Report

Licence Condition

Licence condition 4.2 is drafted to read as:

"The Licence Holder must, by 30 September each year, provide the following documents to the Tribunal in respect of the preceding Financial Year:

1) the compliance report, audit report and certification referred to in condition 4.1; and
2) the report the Licence Holder is required to submit to the relevant Commonwealth regulator under section 30AG of the Security of Critical Infrastructure Act 2018 (Cth)."

Response from Licence Holders

A licence holder has questioned whether IPART is an entity to whom protected information may be disclosed under section 43E of the SOCI Act. This would affect whether the use or disclosure of protected information by IPART is covered by section 44 of the SOCI Act.

CyberCX's Response

CyberCX should seek written advice from the Department of Home Affairs to clarify this matter.

A reading of s43E of the SOCI Act may suggest that IPART is an agency administered by a Minister with responsibility for regulation or oversight of the critical infrastructure sector. Therefore, under this interpretation it could be permissible under s43E(iv) for the licence holders to provide IPART with a copy of the report.

However, IPART should seek clarification from the Department of Home Affairs on this matter. If the Department determines that IPART is not an acceptable entity under s43E of the SOCI Act, then this change should be removed from the IPART licence conditions.

3.4 Definition of 'ICT Infrastructure'

Licence Condition

The relevant portion of licence condition 5.3 reads as:

"ICT Infrastructure means the information and communications technology equipment, systems, firmware and software for handling information and managing communication processes."

Response from Licence Holders

Licence holders have suggested a definition relating to either defining the positive case or defining it by what it is not. For example: 'software and systems used in the operation and control of the network infrastructure used for the conveyance of electricity.'

Further feedback from Licence Holders request that IPART consider specifying that the ICT Infrastructure equipment be defined as that equipment specifically used to manage the Operational Technology that controls the supply of electricity. This is a reasonable distinction given that there is a risk that the definition of ICT Infrastructure could otherwise be misinterpreted beyond the intended scope.

CyberCX's Response

IPART could consider an explicit definition of 'ICT Infrastructure' to achieve a similar effect to the following:

'Information and communications technology equipment, systems, firmware and software directly supporting the Operational Technology environment used for the control of the supply of electricity.'

3.5 Definition of 'Operational Technology'

Licence Condition

There is currently no definition or draft definition for 'operational technology' (OT).

The licence conditions do include the following related definitions in licence condition 5.3:

"Operational Technology Information means all information relating to the operational technology of the System (such as the supervisory control and data acquisition (SCADA) system) and associated ICT Infrastructure including, for example, design specifications and operating manuals.

Operational Technology Responsibility means being responsible for:

(a) delivering the supervisory control and data acquisition (SCADA) capability required to safely and reliably operate the System, and

(b) developing and implementing strategies to manage cyber security and other threats affecting the network operational technology environment, and

(c) developing systems for effectively managing assets remotely, including but not limited to network switches, condition monitoring and remote interrogation or operation of protection systems and relays."

Response from Licence Holders

A licence holder has recommended adding a definition of Operational Technology (OT). The licence holder has suggested the following definition:

'Operational Technology: Technology that directly controls devices on the distribution system and transmission system, including:

a) the SCADA Master Stations and Distribution Management Systems (where they have operational control functionality) and other associated systems that directly control primary equipment on the distribution system; and
b) the ICT infrastructure on which the systems referred to in (a) above operate, the remote devices these systems control, and the associated telecommunication network.'

CyberCX's Response

IPART should consider not limiting the definition of OT to the control of network systems as this would exclude the monitoring of network systems. IPART should consider adding monitoring to the suggested definition.

IPART could consider words to the effect of:

'Technology that directly controls or monitors devices on the distribution system and transmission system, including:

a) the SCADA Master Stations and Distribution Management Systems (where they have operational control functionality) and other associated systems that directly control primary equipment on the distribution system; and
b) the ICT infrastructure on which the systems referred to in (a) above operate, the remote devices these systems control, and the associated telecommunication network.'

3.6 Definitions of 'Third Party Data' and 'Sensitive Information'

Licence Condition

The relevant parts of licence condition 5.3 read as:

"Third Party Data includes:

(a) Communications, within the meaning of the *Telecommunications (Interception and Access) Act 1979* (Cth), and

(b) personal information, within the meaning of the *Privacy Act 1998* (Cth), and

(c) closed-circuit television footage."

And:

"Sensitive Information means:

(a) Operational Technology Information,

(b) Load Data relating to, or obtained in connection with, the operation of the System by a Relevant Person, and

(c) Third Party Data that the Licence Holder obtains or accesses indirectly because a Carrier or another person transferred the Third Party Data using the Licence Holder's infrastructure."

Response from Licence Holders

The licence holders have put forward questions about the definition of third-party data, including:

- Whether the definition of third-party data is limited to data carried over licence holder infrastructure by a Carrier or other third person.
- The definition of 'indirectly'.
- Whether the definition of third-party data includes external parties joining a Zoom call or external consultants logging onto a licence holder's 'guest' Wi-Fi network.
- Whether customer information obtained from a Retailer be considered Third Party Data.
- Whether third-party data includes customer and other external data.
- Whether employee data is included in this definition.

CyberCX's Response

Firstly, the proposed changes include transferring responsibility for the regulation of all personal information and data to the federal regulator – the Office of the Australian Information Commissioner (OAIC) via the *Privacy Act* 1998. This change would suggest that part B of the definition, "personal information, within the meaning of the *Privacy Act 1998* (Cth), and" could be removed.

Secondly, IPART should also consider whether the definition of 'sensitive information' should be restricted from third-party data that the licence holder "obtains or accesses" to something more specific such as third-party data that the licence holder 'stores or processes'.

Thirdly, IPART should consider whether the definition used for 'communications' is too broad in this instance, particularly with concern to the implications for 'sensitive information'.

Finally, while this may be addressed through the second point above, IPART could consider the meaning of the word 'indirectly' in the definition of 'sensitive information'.