Australian Government
Department of Infrastructure, Transport, Regional Development and Communications

Exposure draft:

1. Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022

2. Telecommunications (Carriage Service Provider—Security Information) Determination 2022

Register of critical telecommunications assets and mandatory cyber incident reporting

February 2022

25 February 2022 / INFRASTRUCTURE

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Creative Commons licence

With the exception of (a) the Coat of Arms; (b) the Department of Infrastructure, Transport, Regional Development and Communications photos and graphics; and (c) [OTHER], copyright in this publication is licensed under a Creative Commons Attribution 4.0 Australia Licence.

Creative Commons Attribution 4.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

Further information on the licence terms is available from https://creativecommons.org/licenses/by/4.0/

Use of the Coat of Arms

The Department of the Prime Minister and Cabinet sets the terms under which the Coat of Arms is used. Please refer to the Commonwealth Coat of Arms - Information and Guidelines publication available at http://www.pmc.gov.au.

Contact us

This publication is available in hard copy or PDF format. All other rights are reserved, including in relation to any departmental logos or trade marks which may exist. For enquiries regarding the licence and any use of this publication, please contact:

Director – Creative Services
Communication Branch
Department of Infrastructure, Transport, Regional Development and Communications
GPO Box 594
Canberra ACT 2601
Australia

Email: publishing@infrastructure.gov.au
Website: www.infrastructure.gov.au

Table of contents

Purpose

The Department of Infrastructure, Transport, Regional Development and Communications would like to hear the views of the telecommunications industry and the community on a proposed new carrier licence condition and a new service provider rule for a register of critical telecommunications assets and mandatory reporting of cyber security incidents.

Background

The community expects high standards of security to apply to the telecommunications industry given the importance of telecommunications to the economy and people's everyday lives, and the sensitivity of the information carried across the industry's networks. In addition, other critical infrastructure and services, such as power, financial services and health, rely on telecommunication networks, facilities and systems.

Consequently, failure of the telecommunications networks – because of sabotage, espionage, foreign interference or natural disasters – can have a domino effect, and a very real impact, across society and the economy.

Threats facing the industry, and those that rely on the industry, include possible:

- compromise or degradation of telecommunications networks;
- compromise of valuable data or information of a sensitive nature, such as aggregate stores of personal data or commercial or other sensitive data (including telecommunication companies' own data, and the data transmitted over networks by their customers);
- impairment of the availability or integrity of telecommunications networks; or
- impact on other critical infrastructure or government services (such as banking/finance, health or transport services).

The Australian Government is committed to protecting the essential services Australians rely on by improving the security and resilience of critical infrastructure, including in the telecommunications sector. It is looking to make adjustments to the regulatory arrangements in 2 phases:

- these initial instruments (Phase 1); and
- a forthcoming Phase 2 consultation process about further proposed reform (see below).

Why a new carrier licence condition and service provider rule are needed

As part of the Australian Government's commitment to protecting the essential services that all Australians rely on, the *Security of Critical Infrastructure Act 2018* (SOCI Act) was amended in December 2021. As a result, entities in a wide range of sectors in the economy will have new positive security obligations, including:

- giving the Secretary of the Department of Home Affairs certain information about critical infrastructure assets so it can be included in a register; and
- telling the Australian Signals Directorate if a cyber-security incident has a relevant impact on a critical infrastructure asset.

In order to avoid regulatory duplication and provide clarity for industry, the Government has decided these obligations for the telecommunications sector will be introduced by using mechanisms under the *Telecommunications Act 1997* (Tel Act). The Tel Act contains a well-

established regulatory framework that is familiar to industry and is embedded in how the telecommunications sector operates.

Specifically, as an initial step (Phase 1) the Government is proposing to make a new carrier licence condition and a new service provider rule. The new condition and rule will impose obligations on carriers and eligible carriage service providers that align with the Register of Critical Infrastructure Assets and mandatory cyber-incident reporting obligations other sectors will have under the SOCI Act.

Other powers under Part 3A of the Security of Critical Infrastructure Act 2018

The SOCI Act also gives the Government powers to assist industry in certain situations if a serious cyber-security incident has had, is having or will have a relevant impact on a critical infrastructure asset. These assistance powers will be available for the Government to use in relation to the telecommunications sector under the SOCI Act; they will not be mirrored in the Tel Act.

What the new condition and rule will do

Primarily, the proposed carrier licence condition and service provider rule would require carriers and eligible CSPs to:

- give the Secretary of the Department of Home Affairs operational information in relation to their assets and, where an entity other than the carrier or eligible CSP holds a direct interest in an asset owned or operated by the carrier or eligible CSP, the interest and control information of direct interest holders in the asset;
- give the Australian Signals Directorate (ASD) a notice of a critical cyber security incident no later than 12 hours after the carrier or eligible CSP becomes aware of the incident; and
- give the ASD a notice of other cyber security incidents no later than 72 hours after the carrier or eligible CSP becomes aware of the incident.

Who the new condition and rule will affect

All holders of a carrier licence will be subject to the new carrier licence condition. All eligible CSPs would have to comply with the new service provider rule, unless they are a carrier. Eligible CSPs are defined in section 127 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* as a CSP who supplies a:

- standard telephone service, where any of the customers are residential customers or small business customers;
- public mobile telecommunications service; or
- carriage service that enables end-users to access the internet; or
- carriage service intermediary who arranges for the supply of one of these services.

Eligible CSPs must be members of the Telecommunications Industry Ombudsman scheme. The obligations under the new condition and rule will be administered utilising the existing provisions of the Tel Act.

The estimated cost of the new condition and rule

We would like to understand the estimated costs carriers and eligible CSPs are likely to incur in order to comply the obligations the new condition and rule will introduce. These costs include both initial and on-going capital expenditure and administration costs. This information will help us assess the costs and benefits of the proposed condition and rule and prepare a formal Regulation Impact Statement (RIS).

The information you provide will not be shared with anyone beyond those preparing the RIS. All costing data that will be assessed in the RIS will be at an aggregate level and will not identify individual businesses.

Where you can find the new condition and rule

The new condition and rule are hyperlinked in Appendix A and B at the end of this consultation paper. They are also available through our website - Have your say | Department of Infrastructure, Transport, Regional Development and Communications, Australian Government

Your views count

We would like to know your views on:

1. the proposed new carrier licence condition and new service provider rule for a register of critical telecommunications assets and mandatory reporting of cyber security incidents; and
2. the estimated cost of the complying with these obligation for your organization – after identifying whether you are a carrier or an eligible CSP.

We will take your feedback into account when advising the Minister for Communications, Urban Infrastructure, Cities and the Arts on the content of the new condition and rule.

You can upload written comments on the proposed condition and rule through the page on our website that relate to this consultation - Have your say | Department of Infrastructure, Transport, Regional Development and Communications, Australian Government

Due Date for input: **Close of business: Tuesday, 29 March 2022**

Other reforms

General reforms for Critical Infrastructure

The Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (SLACIP Bill), if passed un-amended by the Parliament, will impose further obligations on critical infrastructure sectors of the economy, including the obligation to prepare and maintain an all hazards risk management program (RMP).

The SLACIP Bill will also give the Minister for Home Affairs the power to declare that a critical infrastructure asset is a system of national significance (SoNS) and to impose enhanced cyber security obligations on the responsible entity for a SoNS.

Longer term telecommunications security reforms (Phase 2)

The Government has decided an equivalent RMP obligation will be applied to the telecommunications industry by making changes to existing arrangements in the Tel Act, rather than by making rules under the SOCI Act. However, the SLACIP Bill's proposed SoNS declaration power and the enhanced cyber security obligations would apply to the telecommunications industry under the SOCI Act.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) released its statutory review into the operation of the Telecommunications Sector Security Reforms (TSSR) in Part 14 of

the Tel Act on 7 February 2022. The Government is now in the process of preparing a response to its six recommendations.

In due course, DITRDC and the Department of Home Affairs will consult with industry and the community on changes to the Tel Act that have an equivalent effect to the RMP requirements of the SOCI Act. At the same time, we will also consult on other potential changes to the Tel Act and its supporting administrative arrangements to both respond to the PJCIS report and ensure the regulation of telecommunication security continues to be fit for purpose.

Appendix A— Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022 (*download link*)

can be downloaded from: https://www.infrastructure.gov.au/tel-sector-security-info-consult

Appendix B— Telecommunications (Carriage Service Provider—Security Information) Determination 2022 (*download link*)

can be downloaded from: https://www.infrastructure.gov.au/tel-sector-security-info-consult