EXPLANATORY STATEMENT

Telecommunications Act 1997

Telecommunications (Carrier License Conditions – Security Information) Declaration 2022

Telecommunications (Carriage Service Provider – Security Information) Determination 2022

Authority

The Minister for Communications, the Hon Michelle Rowland MP, has made the *Telecommunications (Carrier License Conditions – Security Information) Declaration 2022* and the *Telecommunications (Carriage Service Provider – Security Information) Determination 2022* **(the instruments)** under the *Telecommunications Act 1997* (**the Tel Act**).

Section 63(1) of the Tel Act provides that the Minister may, by legislative instrument, declare that carrier licenses be made subject to such conditions as are specified in the instrument.

Section 63(3) provides that the Minister may, by legislative instrument, declare that carrier licenses granted to specified persons during specified period be made subject to such conditions as are specified in the instrument.

Section 99(1A) provides that the Minister may, by legislative instrument, make a determination setting out rules that apply to Carriage Service Providers (**CSPs**) in relation to the supply of specified carriage services – known as a Service Provider Determination.

Purpose and Operation of the Instruments

The instruments impose a new carrier license condition and a new service provider rule for a register of critical telecommunications assets and mandatory reporting of cyber security instruments.

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* (**the SOCI Act**) was amended in December 2021 to expand the obligations and apply these to a wider range of entities. As a result, entities in a wide range of sectors in the economy will have new positive security obligations, including:

1. Giving the Secretary of the Department of Home Affairs certain information about critical infrastructure assets so it can be included in a register; and
2. Informing the Australian Signals Directorate of a cyber-security incident that has had 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* (the 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.

As part of Phase 1 of this process, the new condition and rule impose obligations on carriers and eligible carriage service providers that align with the critical asset register and mandatory cyber-incident reporting obligations other sectors will have under the SOCI Act.

Specific definitions of relevant terminology are incorporated into the instruments for the purposes of clarifying the meaning of:

a) "*unauthorised* access, modification or impairment"

b) "*operational information*"
c) "*interest and control information*"
d) "*direct interest holder*"

(A number of notes also clarify the interaction between these instruments and other Commonwealth laws.)

The carrier license provision and service provider rule will require carriers and CSPs respectively to:

a) provide the Secretary of the Department of Home Affairs (**Home Affairs**) with operational information in relation to their telecommunications 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;
b) provide the Australian Cyber Security Centre of the Australian Signals Directorate (**ASD**) with notice of a critical cyber security incident no later than 12 hours after the carrier or eligible CSP becomes aware of the incident;
c) provide the ASD with notice of other cyber security incidents no later than 72 hours after the carrier or eligible CSP becomes aware of the incident.

The initial obligation of carriers and eligible CSPs to provide the Secretary of Home Affairs with asset information[1] is being aligned with the date on which these obligations come into effect for other sectors. This is 7 October 2022 for new carriers and eligible CSPs, or within the end of 30 days of becoming a carrier or an eligible CSP (as the case may be).

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:

a) standard telephone service, where any of the customers are residential customers or small business customers;
b) public mobile telecommunications service; or
c) carriage service that enables end users to access the internet; or
d) 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 through existing provisions of the Tel Act. This subset of the broader category of CSPs has been chosen as they provide services to the public.

Sunsetting Provisions

It is intended that the obligations in the instruments will, in due time, be incorporated into the Tel Act through a proposed amendment Act that will consolidate and streamline security obligations for the sector. As such, the instruments have been drafted to include sunset clauses to ensure they will cease operation after a period of 18 months.

Compliance Provisions

The Carrier licence conditions and the CSP rules are both subject to a compliance regime, section 68 and section 101 of the Tel Act respectively. This has a direct equivalent in sections 23 and 24 of the SOCI Act, though the penalties for non-compliance differ. The SOCI Act has a fixed civil penalty of 50 penalty units, whereas the Tel Act has a theoretical maximum civil penalty of $10 million for each

[1] This encompasses operational information in relation to each of the assets held and relevant asset and control information of direct interest holders in assets owned or operated by the entity.

contravention if the entity is a body corporate, or $50,000 for each contravention by a person other than a body corporate (section 570 of the Tel Act). It is also important to note that the Federal Court has the discretion to leverage a pecuniary penalty it deems appropriate in the circumstance.[2] In the event that enforcement activity is required during the time these instruments are in force, the intent is that any penalties sought would be in line with those in the SOCI Act

Consultation

Section 64 of the Tel Act requires that carrier licence holders be provided with a draft version of the proposed condition and invite submissions within a period of at least 30 days. This process occurred in February and March 2022. There is no corresponding requirement for consultation on the subject of the service provider rule. Despite this, submissions were sought from eligible CSPs to align with the treatment of carriers.

The Minister has carefully considered responses and incorporated feedback on the instruments and their associated costs into a redraft of the initially proposed instruments. A formal departmental response to this consultation will be made available on the Department's website and the Department will meet with parties that provided input to discuss the contents of the response.

Regulatory Impact Assessment

The Department has published an addendum to the "Protecting Critical Infrastructure and Systems of National Significance regulatory reforms" Regulation Impact Statement. Overall the Department has considered the regulation impact caused by the instruments that have been made and consider that, while there is a financial impact to be borne by the telecommunications sector, this impact is consistent with the regulation impact assessment conducted by Home Affairs attached to the SLACI Bill.

Equivalent Outcomes with the *Security of Critical Infrastructure Act 2018*

It is important to note that the some of the definitions used for the instruments do differ to those in the SOCI Act. The instruments are subordinate to the Tel Act and, therefore are bound by those definitions in the Tel Act as instruments cannot alter these. However, the definitions do not alter the effect or scope of the instruments in a material way to the effect or scope of the SOCI Act. As such the effect and scope, and as a result the impact on the telecommunications sector, is largely the same.

Statement of Compatibility with Human Rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the *Legislation Act 2003* applies to cause a statement of compatibility with human rights to be prepared in respect of that legislative instrument.

The statement of compatibility set out below has been prepared to meet that requirement.

Overview of the Instrument

The instruments are primarily concerned with the introduction of a condition and rule affecting corporate telecommunications entities, their conduct and obligations. The intended purpose of the instruments are to improve the overall security of telecommunications assets, and therefore telecommunications access, in Australia.

Human Rights Implications

The instruments as drafted have an overwhelming positive implication towards human rights. As stated by the United Nations Secretary-General António Guterres[3]:

> *The digital age has opened up new frontiers of human welfare, knowledge and exploration. Digital technologies provide new means to advocate for, defend and exercise our rights.*

Telecommunications networks facilitate the sharing of information which enable an individual's political and social rights, while providing an avenue for the freedom of expression, right to education and work. However, as Secretary-General Guterres argues, there is a propensity for those networks to also be an avenue for the violation of those same rights.

Cyber-attacks and cyber-security incidents have the potential to shut down or restrict access to the internet or other telecommunications networks and may result in the theft of personal details and information. The instruments intend to develop a framework in which the risk of cyber-attacks and cyber-security incidents impinge on an individual's human rights can be mitigated or ameliorated.

Conclusion

By all reasonable inferences, it is likely that the impact of the instruments upon human rights will be minimal. Full implementation is likely to yield benefits to rights considerations through pursuit and protection of objectives which facilitate access to safe and secure telecommunications services and the essential services they enable.

The instrument is compatible with human rights as it does not invoke any issues which may be detrimental to human rights.

[3] Antonio Guterres, 'The Highest Aspiration – A call to action for human rights 2020', United Nations [https://www.un.org/sg/sites/www.un.org.sg/files/atoms/files/The_Highest_Asperation_A_Call_To_Action_For_Human_Right_English.pdf]

APPENDIX A - Detailed explanation of the Instrument

Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022

PART 1 – PRELIMINARY

1 Name of the instrument

Provides the title of the instrument.

2 Commencement

Provides a table of commencement for each part of the instrument. The key dates are 7 July 2022 for the commencement of the cyber security notification obligation and 7 October 2022 for the provision of information for the asset register.

3 Authority

Provides the legislative authority for the instrument.

4 Repeal

Provides the instrument will cease to have effect and be automatically repealed after 18 months.

5 Interpretation

Provides a specific meaning for terms and titles employed in the instrument, including those sharing the same meanings given in related legislation, and specifically the definitions within the SOCI Act.

Many of the defined terms draw on language in the SOCI Act and rules made thereunder, with amendments to align with the terminology used in the Tel Act.

Of particular note are the following definitions:

> ***asset***, which focuses on tangible, real-world assets. While the intent is not to capture all items that may appear in a firms' asset register, the term has been defined widely to ensure that the obligation to report cyber incidents is not constrained. Intangible assets like goodwill, the value of trademarks, and other similar types of intellectual property are not intended to be covered. The term specifically includes computer software (computer programmes) and data as these are critical to cyber security. The term also excludes *customer premises equipment* as even though a carrier may own equipment such as a consumer wifi router, this type of equipment is controlled by the customer rather than the carrier.
>
> ***cyber security incident*** goes beyond the definition within the SOCI Act and includes the unauthorised impairment of an asset used to supply a carriage service (the technical term for a telecommunications service).
>
> ***cloud service*** and ***software-as-a-service*** draw on industry accepted definitions of these services.

6 Specific definition—meaning of *unauthorised* access, modification or impairment

Provides a specific meaning for 'unauthorised' access and 'entitled' access for the purposes of defining a 'cyber security incident'.

Subsection (1) provides that access, modification or impairment is deemed 'unauthorised' if the person causing the access, modification or impairment is not entitled to do so.

Subsection (2) provides that it is immaterial whether the person can be identified.

Subsection (3) provides the criteria under which a person may be deemed 'entitled' to cause that access, modification or impairment.

7 Specific definition—meaning of *operational information*

Provides a specific meaning for 'operational information' in relation to an asset of a carrier.

Subsection (1) provides the specific qualities of an asset which are deemed 'operational information'.

Subsection (2) provides requirements for information to be included in the description of arrangements for maintained data under (1)(e). This obligation extends to computer servers that support cloud services and software-as-a-service arrangements.

8 Specific definition—meaning of *interest and control information*

Provides a specific meaning for 'interest and control information' in relation to a direct interest holder in an asset of a carrier.

Subsection (1) provides specific types of information deemed to be 'interest and control information'.

Subsection (2) provides that information under subsection (1) may include 'personal information' within the meaning of the *Privacy Act 1988*.

9 Specific definition—meaning of *direct interest holder*

Provides a specific meaning for 'direct interest holder' in relation to an asset that is owned or operated by a carrier.

Subsection (1) provides that the general definition of a 'direct interest holder' is an entity which holds an interest of at least 10% in the asset, or holds an interest in the asset that puts the entity in a position to influence or control the asset.

Subsection (2) provides that interests in assets held by a Governor, First Minister, Administrator, or Minister of a State or Territory are excluded from the general definition.

Subsection (3) provides further circumstances where the general definition of subsection (1) will not apply.

Subsection (4) provides (without limitation) the circumstances in which interests in assets owned or operated by a carrier are deemed to be 'held'.

PART 2 – CONDITIONS

10 Carrier licence conditions

Provides the scope of compliance for conditions within the instrument from its commencement for carrier license holders.

Subsection (1) provides that persons holding a carrier license at the time of commencement must comply with conditions specified in sections 10, 11, 12 and 13 at all times during which they are a carrier.

Subsection (2) provides that persons granted a carrier license after the instrument commences must comply with conditions specified in sections 10, 11, 12 and 13 at all times during which they are a carrier.

11 Notification of critical cyber security incidents

Creates a condition requiring that carriers notify the Australian Signals Directorate (ASD) of certain critical cyber security incidents.

Subsection (1) creates a requirement that, subject to subsection (5), carriers provide the ASD with a report of cyber security incidents that have had or are having a significant impact on the availability of any of its assets as soon as practicable and within 12 hours of the carrier becoming aware of the incident.

Subsection (2) provides that a security incident is deemed to have a 'significant impact' on the availability of an asset only if it is both used in connection with provision of essential goods and service and if the incident has materially disrupted the availability of those goods or services. The intent is only to capture those goods or services that are critical to the health, safety, or good order of the Australian community.

Subsection (3) provides that reports under subsection (1) may be given orally or in writing, in the approved form.

Subsection (4) provides standards for oral reports of the type described in subsection (3).

Subsection (5) provides that the obligation under subsection (1) will not apply in respect of a cyber security incident in the presence of appropriate advice in writing from an ASD officer advising that a report is not required. Such a notice is not a legislative instrument.

12 Notification of other cyber security incidents

Creates a condition requiring that carriers notify the ASD of certain other cyber security incidents.

Subsection (1) creates a requirement that, subject to subsection (5), carriers provide the ASD with a report of cyber security incidents that have had or are having a relevant impact on the availability of any of its assets as soon as practicable and within 72 hours of the carrier becoming aware of the incident.

Subsection (2) provides specific criteria for circumstances in which a cyber security incident will be deemed to have had a 'relevant impact' on an asset – including where the availability, integrity, reliability or confidentiality of the asset is affected.

Subsection (3) provides that reports under subsection (1) may be given orally or in writing, in the approved form.

Subsection (4) provides standards for follow up written reports to oral reports described in subsection (3).

Subsection (5) provides that the obligation under subsection (1) will not apply in respect of a cyber security incident in the presence of appropriate advice in writing from an ASD officer advising that a report is not required. This is intended to permit a carrier to contact ASD to confirm whether a report is required, and to allow them to rely upon advice – eg in an email – that nothing is required for that event.

13 Initial obligation to give information

Creates a condition requiring that carriers provide the Home Affairs Secretary (the Secretary) with certain information about the carrier in writing.

Subsection (1) provides that carriers must provide the Secretary with operational information in relation to each asset of the carrier, and information about the interest and control and control

information of direct interest holders in the asset. It should be noted that carriers have an obligation to report all this information, and that unlike the similar obligation in the SOCI Act, there is no obligation on direct interest holders to report interest and control information as well.

Subsection (2) provides that the information referred to in subsection (1) must be given in the approved form and by the later of the day on which this part of the instrument commences (7 October 2022) and 30 days after being licensed as a carrier.

Subsection (3) directs carriers to provide operational information at the level of component systems etc, as the intent is to develop a register that draws upon material information about carrier operations and not to collect details on every item owned by a carrier.

14 Ongoing obligation to give information and notify of events

Creates a condition requiring that carriers provide the Secretary with information relating to and give notice of certain events.

Subsection (1) provides that, subject to subsection (3) and section 14, if carriers are required to give information in accordance with subsection (2), the carrier must provide that information in the approved form and within 30 days of the event occurring.

Subsection (2) provides a table specifying the nature of the obligation to give certain types of information in specific circumstances. In essence this requires correcting information supplied after the listed events.

Subsection (3) provides that subsection (1) will not apply if a second notifiable event occurs within 30 days of the first event and where as a result of the second event any information that was subject to the requirement to provide is no longer correct.

Subsection (4) provides that the obligation under subsection (1) will not apply in respect to an asset if the Secretary advised in writing that a report is not required. This is intended to permit a carrier to confirm whether an update is required, and to allow the carrier to rely upon advice – eg in an email – that nothing is required.

15 Circumstances where the information is not able to be obtained

Provides that section 12 and section 13 do not apply if the carrier has used its best endeavours to obtain the required information to no avail.

APPENDIX B - Detailed explanation of the Instrument

Telecommunications (Carriage Service Provider—Security Information) Determination 2022

PART 1 – PRELIMINARY

1 Name of the instrument

Provides the title of the instrument.

2 Commencement

Provides a table of commencement for each part of the instrument. The key dates are 7 July 2022 for the commencement of the cyber security notification obligation and 7 October 2022 for the provision of information for the asset register.

3 Authority

Provides the legislative authority for the instrument.

4 Repeal

Provides the instrument will cease to have effect and be automatically repealed after 18 months.

5 Interpretation

Provides a specific meaning for terms and titles employed in the instrument, including those sharing the same meanings given in related legislation, and specifically the definitions within the SOCI Act.

Many of the defined terms draw on language in the SOCI Act and rules made thereunder, with adjustments to align with the terminology used in the Tel Act.

Of particular note are the following definitions:

> ***asset***, which focuses on tangible, real-world assets. While the intent is not to capture all items that may appear in a firms' asset register, the term has been defined widely to ensure that the obligation to report cyber incidents is not constrained. Intangible assets like goodwill, the value of trademarks, and other similar types of intellectual property are not intended to be covered. The term specifically includes computer software (computer programmes) and data as these are critical to cyber security. The term also excludes *customer premises equipment* as even though an eligible carriage service provider may own equipment such as a consumer wifi router, this type of equipment is controlled by the customer rather than the carriage service provider.
>
> ***cyber security incident*** goes beyond the definition within the SOCI Act and includes the unauthorised impairment of an asset used to supply a carriage service (the technical term for a telecommunications service) by the eligible carriage service provider. This is narrower than the equivalent provision for a carrier, reflecting the fact that such service providers generally have few physical assets and generally utilise the assets of licenced carriers.
>
> ***eligible carriage service provider*** has the same meaning as that term in s.127 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*. This is the provision that requires standard telephone service providers, public mobile telecommunications providers and internet service providers, or any body that arranges supply of these services, to be registered with the Telecommunications Industry Ombudsman.
>
> ***cloud service*** and ***software-as-a-service*** draw on industry accepted definitions of these services.

6 Specific definition—meaning of *unauthorised* access, modification or impairment

Provides a specific meaning for 'unauthorised' access and 'entitled' access for the purposes of defining a 'cyber security incident'.

Subsection (1) provides that access, modification or impairment is deemed 'unauthorised' if the person causing the access, modification or impairment is not entitled to do so.

Subsection (2) provides that it is immaterial whether the person can be identified.

Subsection (3) provides the criteria under which a person may be deemed 'entitled' to cause that access, modification or impairment.

7 Specific definition—meaning of *operational information*

Provides a specific meaning for 'operational information' in relation to an asset of an eligible carriage service provider.

Subsection (1) provides the specific qualities of an asset which are deemed 'operational information'.

Subsection (2) provides requirements for information to be included in the description of arrangements for maintained data under (1)(e). This obligation extends to computer servers that support cloud services and software-as-a-service arrangements.

8 Specific definition—meaning of *interest and control information*

Provides a specific meaning for 'interest and control information' in relation to a direct interest holder in an asset of an eligible carriage service provider.

Subsection (1) provides specific types of information deemed to be 'interest and control information'.

Subsection (2) provides that information under subsection (1) may include 'personal information' within the meaning of the *Privacy Act 1988*.

9 Specific definition—meaning of *direct interest holder*

Provides a specific meaning for 'direct interest holder' in relation to an asset that is owned or operated by an eligible carriage service provider.

Subsection (1) provides that the general definition of a 'direct interest holder' is an entity which holds an interest of at least 10% in the asset, or holds an interest in the asset that puts the entity in a position to influence or control the asset.

Subsection (2) provides that interests in assets held by a Governor, First Minister, Administrator, or Minister of a State or Territory are excluded from the general definition.

Subsection (3) provides further circumstances where the general definition of subsection (1) will not apply.

Subsection (4) provides (without limitation) the circumstances in which interests in assets owned or operated by an eligible carriage service provider are deemed to be 'held'.

PART 2 – RULES

10 Application

Provides that the instrument applies, for the purposes of subsection 99(1A) of the *Telecommunications Act,* to each eligible carriage service provider who is not a carrier in relation to

the supply of standard telephone services for residential and small business customers, public mobile telecommunications services, and carriage services that enables end-users to access the internet.

11 Notification of critical cyber security incidents

Creates a rule that eligible carriage service providers who become aware of cyber security incidents must provide a report of the incident to the Australian Signals Directorate (the ASD).

Subsection (1) provides that carriage service providers must provide the ASD with a report of cyber security incidents that have had or are having a significant impact on the availability of any of its assets as soon as practicable, and within 12 hours of the carriage service provider becoming aware of the incident.'

Subsection (2) provides that incidents will be deemed to have had a 'significant impact' where the asset is used in connection with the provision of essential goods or services and the incident has materially disrupted the availability of those essential goods or services. The intent is only to capture those goods or services that are critical to the health, safety, or good order of the Australian community.

Subsection (3) provides that reports to the ASD may be given orally or in writing in the approved form.

Subsection (4) provides that where reports are given orally the carriage service provider must make a written copy of the report in the approved form and give a written copy to the ASD within 84 hours of the original report being given.

Subsection (5) provides that the obligation under subsection (1) will not apply in respect of a cyber security incident in the presence of appropriate advice in writing from an ASD officer advising that a report is not required. Such a notice is not a legislative instrument.

12 Notification of other cyber security incidents

Creates a rule requiring that carriage service providers notify the ASD of certain other cyber security incidents.

Subsection (1) creates a requirement that, subject to subsection (5), eligible carriage service providers provide the ASD with a report of cyber security incidents that have had or are having a relevant impact on the availability of any of its assets as soon as practicable and within 72 hours of the carriage service provider becoming aware of the incident.

Subsection (2) provides specific criteria for circumstances in which a cyber security incident will be deemed to have had a 'relevant impact' on an asset – including where the availability, integrity, reliability or confidentiality of the asset is affected.

Subsection (3) provides that reports under subsection (1) may be given orally or in writing, in the approved form.

Subsection (4) provides standards for follow up written reports to oral reports described in subsection (3).

Subsection (5) provides that the obligation under subsection (1) will not apply in respect of a cyber security incident in the presence of appropriate advice in writing from an ASD officer advising that a report is not required. This is intended to permit an eligible carriage service provider to contact ASD to confirm whether a report is required, and to allow them to rely upon advice – eg in an email – that nothing is required for that event.

13 Initial obligation to give information

Creates a rule requiring that eligible carriage service providers provide the Home Affairs Secretary (the Secretary) with certain information in writing.

Subsection (1) provides that eligible carriage service providers must provide the Secretary with operational information in relation to each asset of the eligible carriage service provider, and information about the interest and control and control information of direct interest holders in the asset. It should be noted that eligible carriage service providers have an obligation to report all this information, and that unlike the similar obligation in the SOCI Act, there is no obligation on direct interest holders to report interest and control information as well.

Subsection (2) provides that the information referred to in subsection (1) must be given in the approved form and by the later of six months after the day on which the instrument commences and 30 days after commencing business as an eligible carriage service provider.

Subsection (3) directs eligible carriage service providers to provide operational information at the level of component systems (such as its control and administrative systems), as the intent is to develop a register that draws upon material information about its operations and not to collect details on every item owned by the firm.

14 Ongoing obligation to give information and notify of events

Creates a rule requiring that carriage service providers provide the Secretary with information relating to and give notice of certain events.

Subsection (1) provides that, subject to subsection (3) and section 14, if eligible carriage service providers are required to give information in accordance with subsection (2), the eligible carriage service provider must provide that information in the approved form and within 30 days of the event occurring.

Subsection (2) provides a table specifying the nature of the obligation to give certain types of information in specific circumstances.

Subsection (3) provides that subsection (1) will not apply if a second notifiable event occurs within 30 days of the first event and where as a result of the second event any information that was subject to the requirement to provide is no longer correct.

Subsection (4) provides that the obligation under subsection (1) will not apply in respect to an asset if the Secretary advised in writing that a report is not required. This is intended to permit an eligible carriage service provider to confirm whether an update is required, and to allow the firm to rely upon advice – eg in an email – that nothing is required.

15 Circumstances where the information is not able to be obtained

Provides that section 12 and section 13 do not apply if the eligible carriage service provider has used its best endeavours to obtain the required information to no avail.