Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024

No. 100, 2024

An Act to amend the law relating to critical infrastructure and telecommunications, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024

No. 100, 2024

An Act to amend the law relating to critical infrastructure and telecommunications, and for related purposes

[*Assented to 29 November 2024*]

The Parliament of Australia enacts:

1 Short title

This Act is the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	29 November 2024
2. Schedules 1 to 4	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
3. Schedule 5, Parts 1 and 2	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
4. Schedule 5, Part 3, Division 1	The later of: (a) immediately after the commencement of the provisions covered by table item 2; and (b) immediately after the commencement of the provisions covered by table item 3.	

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
5. Schedule 5, Part 3, Division 2	At the same time as the provisions covered by table item 3. However, the provisions do not commence at all if Schedule 4 to the *Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2024* does not commence before that time.	
6. Schedule 5, Part 3, Division 3	Immediately before the commencement of Schedule 4 to the *Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2024*. However, the provisions do not commence at all if that Schedule commences before the commencement of the provisions covered by table item 3.	Never commenced
7. Schedule 5, Part 4	At the same time as the provisions covered by table item 3.	
8. Schedule 6	At the same time as the provisions covered by table item 2.	
9. Schedule 7	The day after this Act receives the Royal Assent.	30 November 2024
10. Schedule 8	At the same time as the provisions covered by table item 2.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Data storage systems that hold business critical data

Security of Critical Infrastructure Act 2018

1 Subsection 9(1) (note)

Omit "Note", substitute "Note 1".

2 At the end of subsection 9(1)

Add:

Note 2: Data storage systems that store or process business critical data are part of the critical infrastructure asset: see subsection (7).

3 At the end of section 9

Add:

Data storage systems

(7) If, under this section, an asset is a critical infrastructure asset, then a data storage system in respect of which all of the following requirements are satisfied is taken to be part of the critical infrastructure asset:

(a) the responsible entity for the critical infrastructure asset owns or operates the data storage system;

(b) the data storage system is used, or is to be used, in connection with the critical infrastructure asset;

(c) business critical data is stored, or is processed in or by, the data storage system (whether or not other information is also stored, or is processed in or by, the data storage system);

(d) for a hazard where there is a material risk that the occurrence of the hazard could have an impact on the data storage system, there is also a material risk that the occurrence of the hazard could have a relevant impact on the critical infrastructure asset.

Note: The effect of this subsection is, for example, that:

(a) obligations under Part 2 in relation to a critical infrastructure asset will also need to take into account the data storage system; and

(b) a critical infrastructure risk management program under Part 2A in relation to a critical infrastructure asset will also need to cover the data storage system; and

(c) notification obligations under Part 2B of cyber security incidents relating to any relevant impact on a critical infrastructure asset will also need to take into account any relevant impact on the data storage system.

4 Application provision

The amendments made by this Schedule apply in relation to the following:

(a) assets that are critical infrastructure assets (including systems of national significance) immediately before the commencement of this item;

(b) assets that become critical infrastructure assets (including systems of national significance) on or after the day on which this item commences;

whether the data storage systems came into existence before, on or after the day on which this item commences.

Schedule 2—Managing consequences of impacts of incidents on critical infrastructure assets

Security of Critical Infrastructure Act 2018

1 Paragraph 3(e)

Omit "serious cyber security incidents", substitute "serious incidents relating to critical infrastructure assets".

2 Section 4

Omit "serious cyber security incidents", substitute "a serious incident that has had, is having, or is likely to have, one or more relevant impacts on one or more critical infrastructure assets".

3 Subsections 8G(2) and (3)

Omit "a cyber security incident", substitute "an incident (including a cyber security incident)".

4 Section 12P (heading)

Omit "**a cyber security incident**", substitute "**an incident (including a cyber security incident)**".

5 Section 12P

Omit "a cyber security incident", substitute "an incident (including a cyber security incident)".

6 Part 3A (heading)

Repeal the heading, substitute:

Part 3A—Responding to serious incidents

7 Section 35AA

Repeal the section, substitute:

35AA Simplified outline of this Part

- This Part sets up a regime for the Commonwealth to respond to a serious incident that has had, is having, or is likely to have, one or more relevant impacts on one or more critical infrastructure assets.
- The Minister may, in order to respond to the incident, do any or all of the following things:
  - (a) authorise the Secretary to give information-gathering directions to relevant entities for the assets;
  - (b) authorise the Secretary to give action directions to relevant entities for the assets;
  - (c) if the incident is a cyber security incident—authorise the Secretary to give intervention requests to the authorised agency.
- An information-gathering direction requires the relevant entities to give information to the Secretary.
- An action direction requires the relevant entities to do, or refrain from doing, a specified act or thing.
- An intervention request is a request that the authorised agency do one or more specified acts or things in relation to the assets.

8 Division 2 of Part 3A (heading)

Repeal the heading, substitute:

Division 2—Ministerial authorisation relating to serious incidents

9 Paragraph 35AB(1)(a)

Omit “a cyber security incident”, substitute “an incident”.

10 Paragraph 35AB(1)(b)

Omit "a relevant impact on a critical infrastructure asset (the ***primary asset***)", substitute "one or more relevant impacts on one or more critical infrastructure assets (each of which is a ***primary asset***)".

11 Paragraph 35AB(1A)(a)

Omit "a cyber security incident", substitute "an incident".

12 Paragraph 35AB(1A)(b)

Omit "a relevant impact on a critical infrastructure asset (the ***primary asset***)", substitute "one or more relevant impacts on one or more critical infrastructure assets (each of which is a ***primary asset***)".

13 Paragraph 35AB(2)(a)

Omit "to a specified entity under section 35AK that relate to the incident and the primary asset", substitute "under section 35AK, relating to the incident and one or more primary assets, to one or more relevant entities".

14 Paragraph 35AB(2)(b)

Omit "to a specified entity under section 35AK that relate to the incident and a specified critical infrastructure sector asset", substitute "under section 35AK, relating to the incident and one or more specified critical infrastructure sector assets, to one or more relevant entities".

15 Paragraph 35AB(2)(c)

Omit "a specified entity a specified direction under section 35AQ that relates to the incident and the primary asset", substitute "one or more specified entities a specified direction under section 35AQ that relates to the incident and one or more specified primary assets".

16 Paragraph 35AB(2)(d)

Omit "a specified entity a specified direction under section 35AQ that relates to the incident and a specified critical infrastructure sector asset", substitute "one or more specified entities a specified direction under section 35AQ that relates to the incident and one or more specified critical infrastructure sector assets".

17 Paragraph 35AB(2)(e)

Omit "a specified request under section 35AX that relates to the incident and the primary asset", substitute "one or more specified requests under section 35AX that relate to the incident and one or more specified primary assets".

18 Paragraph 35AB(2)(f)

Omit "a specified request under section 35AX that relates to the incident and a specified critical infrastructure sector asset", substitute "one or more specified requests under section 35AX that relate to the incident and one or more specified critical infrastructure sector assets".

19 Subsection 35AB(2) (at the end of note 3)

Add "The Minister must not give an authorisation under paragraph (2)(e) or (f) unless the Minister is satisfied that the incident is a cyber security incident: see subsection (10).".

20 Paragraph 35AB(5)(a)

After "the asset", insert "or assets".

21 Subsection 35AB(7)

After "paragraph (2)(c) or (d)", insert "in relation to a specified entity".

22 Subsection 35AB(7) (note)

Omit "a cyber security incident", substitute "an incident (including a cyber security incident)".

23 Subparagraph 35AB(8)(a)(ii)

After "the asset", insert "or assets".

24 Subsection 35AB(9)

After "paragraph (2)(c) or (d)", insert "in relation to a specified entity".

25 After subsection 35AB(9)

Insert:

(9A) Without limiting paragraph (2)(c) or (d), a direction referred to in that paragraph may require a specified entity to disclose specified

personal information (within the meaning of the *Privacy Act 1988*) held by the entity to another specified entity for a specified purpose.

(9B) However, the Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d), to the extent that it authorises the giving of a direction covered by subsection (9A), unless the Minister has obtained the agreement of the Minister administering the *Privacy Act 1988*.

26 Subsection 35AB(10)

After "paragraph (2)(e) or (f)", insert "that relates to the incident and an asset".

27 Before paragraph 35AB(10)(a)

Insert:

(aa) the incident is a cyber security incident; and

28 Paragraphs 35AB(10)(b) and (c)

Omit "concerned".

29 Paragraph 35AB(11)(a)

Omit "concerned".

30 Section 35AC

Omit "to a Ministerial authorisation of a request", substitute "to a proposed Ministerial authorisation under paragraph 35AB(2)(e) or (f) in relation to an asset".

31 Paragraphs 35AC(a) to (j)

Omit "to which the Ministerial authorisation relates" (wherever occurring).

32 Subsection 35AD(1)

After "paragraph 35AB(2)(c) or (d)", insert "in relation to an entity".

33 Paragraphs 35AE(2)(a), (3)(a), (4)(a), (5)(a), (6)(a), (7)(a) and (8)(a)

Omit "a cyber security incident", substitute "an incident".

34 Paragraph 35AF(2)(a)

Omit "a cyber security incident", substitute "an incident".

35 Paragraph 35AG(1)(a)

Omit "a cyber security incident", substitute "an incident".

36 Paragraphs 35AH(1)(a), (6)(a) and (7)(a)

Omit "a cyber security incident", substitute "an incident".

37 Paragraph 35AK(1)(a)

Omit "a cyber security incident", substitute "an incident".

38 Subsection 35AQ(2) (note)

Omit "a cyber security incident", substitute "an incident that has had, is having, or is likely to have, a relevant impact on one or more critical infrastructure assets".

39 Subsection 35AS(3)

Omit "cyber security incident", substitute "incident".

40 Subsection 35AX(2) (note)

Omit "section 35AB", substitute "subsection 35AB(10)".

41 At the end of subsection 35BA(1)

Add "and an asset".

42 Subsection 35BK(1)

Omit "a cyber security incident", substitute "an incident".

43 Application and saving provisions

(1) The amendments of Part 3A of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to the giving of an authorisation under subsection 35AB(2) of that Act on or after the day

on which this item commences in relation to an application by the Secretary under that subsection on or after that day.

(2) The *Security of Critical Infrastructure Act 2018*, as in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to the following:

(a) an authorisation given under subsection 35AB(2) of that Act before the day on which this item commences;

(b) an application by the Secretary under that subsection before that day.

Schedule 3—Use and disclosure of protected information

Security of Critical Infrastructure Act 2018

1 Section 4

Omit "Certain information obtained or generated under, or relating to the operation of, this Act is protected information", substitute "Certain documents or information obtained, generated or adopted under, or relating to the operation of, this Act is protected information".

2 Section 5

Insert:

authorised APS employee means an APS employee in the Department in respect of whom an authorisation under section 44A is in force.

confidential commercial information means the following:

(a) information relating to trade secrets;

(b) other information that has a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were communicated.

3 Section 5 (definition of *protected information*)

Repeal the definition, substitute:

protected information has the meaning given by section 5A.

4 Section 5

Insert:

relevant information has the meaning given by section 5A.

5 Section 5 (paragraph (a) of the definition of *security*)

Repeal the paragraph, substitute:

(a) subject to paragraph (b)—has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*; and

6 Section 5 (paragraph (b) of the definition of *security*)

Omit "definition of ***critical energy market operator asset***", substitute "definitions of ***critical energy market operator asset*** and ***protected information***".

7 Section 5 (paragraph (b) of the definition of *security*)

Omit "and 30CW", substitute ", 30CW and 42AA".

8 After section 5

Insert:

5A Meaning of *protected information* and *relevant information*

Protected information

(1) ***Protected information*** is relevant information:

(a) the disclosure of which would or could reasonably be expected to prejudice national security or the defence of Australia; or

(b) the disclosure of which would or could reasonably be expected to prejudice the social or economic stability of Australia or its people; or

(c) that contains, or is, confidential commercial information; or

(d) the disclosure of which would or could reasonably be expected to prejudice the availability, integrity, reliability or security of a critical infrastructure asset.

(2) A document or information is ***protected information*** if it:

(a) was a document or information to which subsection (1) applied; and

(b) is obtained by a person by way of an authorised disclosure under Division 3 of Part 4 or in accordance with section 46.

Relevant information

(3) ***Relevant information*** is:

(a) a document or information that is obtained or generated by a person in the course of exercising powers, or performing duties or functions, under this Act; or

(b) a document or information that is obtained, generated or adopted by an entity for the purposes of complying with this Act;

including, but not limited to, a document or information that:

(c) records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset; or

(d) records or is the fact that an asset is declared under section 52B to be a system of national significance; or

(e) records or is the fact that the Minister has:

(i) given a Ministerial authorisation; or

(ii) revoked a Ministerial authorisation; or

(f) is, or is included in, a critical infrastructure risk management program that is adopted by an entity in compliance with section 30AC; or

(g) is, or is included in, a report that is given under section 30AG or 30AQ; or

(h) is, or is included in, a report under section 30BC or 30BD; or

(i) is, or is included in, an incident response plan adopted by an entity in compliance with section 30CD; or

(j) is, or is included in, an evaluation report prepared under section 30CQ or 30CR; or

(k) is, or is included in, a vulnerability assessment report prepared under section 30CZ; or

(l) is, or is included in, a report prepared in compliance with:

(i) a system information periodic reporting notice; or

(ii) a system information event-based reporting notice; or

(m) records or is the fact that the Minister has:

(i) given a direction under subsection 32(2); or

(ii) revoked such a direction; or

(n) records or is the fact that the Secretary has:

(i) given a direction under section 35AK; or

(ii) revoked such a direction; or

(o) records or is the fact that the Secretary has:

(i) given a direction under section 35AQ; or

(ii) revoked such a direction; or

(p) records or is the fact that the Secretary has:

(i) given a request under section 35AX; or
(ii) revoked such a request.

9 Section 36 (note)

Omit "section 5", substitute "section 5A".

10 Subsections 42(1) and (2)

After "Secretary", insert ", or an authorised APS employee,".

11 After subparagraph 42(2)(a)(vii)

Insert:

(viia) emergency management;

12 Paragraph 42(2)(b)

Repeal the paragraph, substitute:

(b) a Minister of a State, the Australian Capital Territory, or the Northern Territory, who has responsibility for:
(i) law enforcement; or
(ii) emergency management; or
(iii) the regulation or oversight of the relevant critical infrastructure sector to which the protected information relates;

13 At the end of section 42

Add:

(3) An authorised APS employee may disclose protected information under this section, and make a record of or use protected information for the purpose of that disclosure, only if doing so is in accordance with an authorisation under section 44A.

14 After section 42

Insert:

42AA Authorised use and disclosure—availability, integrity, reliability or security of a critical infrastructure asset

A relevant entity (other than the Commonwealth) for a critical infrastructure asset may make a record of, use or disclose protected information if the entity makes the record, or uses or discloses the information:

(a) for a purpose relating to the continued operation of the critical infrastructure asset; or

(b) to mitigate a risk to the availability, integrity, reliability or security of the critical infrastructure asset.

Note: This section is an authorisation for the purposes of other laws, including the Australian Privacy Principles.

15 Section 42A

Before "The", insert "(1)".

16 Section 42A

After "Secretary", insert ", or an authorised APS employee,".

17 At the end of section 42A

Add:

(2) An authorised APS employee may disclose protected information under this section, and make a record of or use protected information for the purpose of that disclosure, only if doing so is in accordance with an authorisation under section 44A.

18 Section 43

Before "The", insert "(1)".

19 Section 43

After "Secretary", insert ", or an authorised APS employee,".

20 At the end of section 43

Add:

(2) An authorised APS employee may disclose protected information under this section only if doing so is in accordance with an authorisation under section 44A.

21 Section 43AA

Before "The", insert "(1)".

22 Section 43AA

After "Secretary", insert ", or an authorised APS employee,".

23 At the end of section 43AA

Add:

(2) An authorised APS employee may disclose protected information under this section, and make a record of or use protected information for the purpose of that disclosure, only if doing so is in accordance with an authorisation under section 44A.

24 Section 43A

Before "The", insert "(1)".

25 Section 43A

After "Secretary", insert ", an authorised APS employee or any other entity".

26 At the end of section 43A

Add:

(2) An authorised APS employee may disclose protected information under this section, and make a record of or use protected information for the purpose of that disclosure, only if doing so is in accordance with an authorisation under section 44A.

27 Subparagraphs 43E(1)(b)(i) and (ii)

After "responsibility for", insert "emergency management or for".

28 Subsections 43E(2) and (3)

Repeal the subsections, substitute:

(2) An entity may disclose protected information if:
(a) the entity is the entity to whom the protected information relates; and
(b) the Secretary has consented, in writing, to the disclosure; and
(c) if the Secretary's consent is subject to one or more conditions—those conditions are satisfied.

Note: This subsection is an authorisation for the purposes of other laws, including the Australian Privacy Principles.

29 After section 43E

Insert:

43F Authorised use and disclosure—relevant entity's business, professional, commercial or financial affairs

A relevant entity for a critical infrastructure asset may make a record of, use or disclose protected information if:
(a) the protected information was obtained, generated or adopted by the entity for the purposes of complying with this Act; and
(b) the entity makes the record, or uses or discloses the information, for the entity's business, professional, commercial or financial affairs.

Note: This section is an authorisation for the purposes of other laws, including the Australian Privacy Principles.

30 At the end of Subdivision A of Division 3 of Part 4

Add:

44A Authorised APS employees

(1) The Secretary may, in writing, authorise an APS employee in the Department, or each APS employee in the Department included in a specified class of APS employees in the Department, to be an authorised APS employee for the purposes of this Subdivision.

(2) The Secretary must, in any authorisation under subsection (1), specify the kind of protected information that the APS employee, or each APS employee in that class, is authorised:
(a) to disclose under section 42, 42A, 43, 43AA or 43A; and

(b) to make a record of or use for the purpose of a disclosure under section 42, 42A, 43AA or 43A.

31 Paragraph 45(1)(a)

Repeal the paragraph, substitute:

(a) the entity obtains, generates or adopts a document or information; and

32 Paragraph 45(1)(b)

After "the", insert "document or".

33 Paragraph 45(1)(c)

After "uses the", insert "document or".

34 Subsection 45(1) (note 2)

Repeal the note, substitute:

Note 2: A document or information that records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset may be protected information: see section 5A.

35 Application provision

The amendments of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to the making of a record, use or disclosure of a document or information on or after the day on which this item commences, whether the document or information is obtained, generated or adopted before, on or after that day.

Schedule 4—Direction to vary critical infrastructure risk management program

Security of Critical Infrastructure Act 2018

1 Section 5

Insert:

relevant official has the meaning given by section 30AI.

serious deficiency has the meaning given by section 30AI.

2 Before paragraph 30AG(2)(e)

Insert:

(db) if the entity was given a direction under section 30AI during the relevant period—includes a statement that:

(i) sets out the content of the direction; and

(ii) sets out how the program was varied in response to the direction; and

3 After section 30AH

Insert:

30AI Direction to vary critical infrastructure risk management program

(1) A relevant official may give the responsible entity for one or more critical infrastructure assets a written direction to vary the entity's critical infrastructure risk management program if the relevant official is satisfied that there are one or more serious deficiencies with the program.

(2) A ***relevant official*** is:

(a) the Secretary, unless paragraph (b) applies; or

(b) if there is a relevant Commonwealth regulator that has functions relating to the security of those assets:

(i) the chief executive officer (however described) of that regulator; or

(ii) an SES employee, or an acting SES employee, in that regulator; or

(iii) a person who holds, or is acting in, a position in that regulator that is equivalent to, or higher than, a position occupied by an SES employee in the Department.

(3) A ***serious deficiency*** is a deficiency that poses a material risk to:

(a) national security; or

(b) the defence of Australia; or

(c) the social or economic stability of Australia or its people.

Contents of direction

(4) A direction under subsection (1) must:

(a) specify the serious deficiencies; and

(b) require the responsible entity to vary the entity's critical infrastructure risk management program to address those deficiencies; and

(c) specify the period within which the responsible entity must vary that program, which must be a period of at least 14 days starting on the day on which the direction is given.

Compliance with direction

(5) The responsible entity must comply with a direction under subsection (1).

Note: If the entity is not a legal person, see Division 2 of Part 7.

Civil penalty: 250 penalty units.

Consultation before giving direction

(6) A relevant official must, before giving a direction under subsection (1), give the responsible entity a written notice:

(a) stating that the relevant official is considering giving the responsible entity a direction under subsection (1); and

(b) specifying the serious deficiencies covered by subsection (1); and

(c) invite the responsible entity to give the relevant official, within 14 days after the day the notice is given to the responsible entity, a written submission in relation to the notice.

(7) A relevant official must, in deciding whether to give a direction under subsection (1), have regard to:

(a) any written submission received from the responsible entity within that 14-day period; and

(b) any action that is taken, or proposed to be taken, by the responsible entity in response to the notice and that is notified to the relevant official within that 14-day period.

(8) Subsection (7) does not limit the matters to which the relevant official may have regard.

Certain persons to give copy of direction to Secretary

(9) A relevant official covered by paragraph (2)(b) must give the Secretary a copy of any direction the relevant official gives under subsection (1).

Direction not a legislative instrument

(10) A direction under subsection (1) is not a legislative instrument.

4 After paragraph 60(2)(g)

Insert:

(gaa) the number of directions given to entities under section 30AI during the financial year; and

5 Application provisions

(1) The amendments of sections 30AG and 60 of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to a financial year that ends after the day on which this item commences.

(2) Section 30AI of the *Security of Critical Infrastructure Act 2018*, as inserted by this Schedule, applies in relation to a direction given on or after the day on which this item commences, whether the critical infrastructure risk management program was adopted before, on or after that day.

Schedule 5—Security regulation for critical telecommunications assets

Part 1—Main amendments

Security of Critical Infrastructure Act 2018

1 After paragraph 3(d)

Insert:

(da) imposing enhanced security obligations on responsible entities for critical telecommunications assets; and

2 Section 4

After:

(d)	imposing enhanced cyber security obligations that relate to systems of national significance;

insert:

(da)	imposing enhanced security obligations for critical telecommunications assets;

3 Section 5

Insert:

Australian waters has the same meaning as in Schedule 3A to the *Telecommunications Act 1997*.

4 Section 5 (note to the definition of *critical public transport asset*)

Omit "Note", substitute "Note 1".

5 Section 5 (at the end of the definition of *critical public transport asset*)

Add:

Note 2: A critical public transport asset that is owned or operated by a carrier may also be a critical telecommunications asset.

6 Section 5 (paragraph (b) of the definition of *critical telecommunications asset*)

Repeal the paragraph, substitute:

(b) any other asset that is:

(i) owned or operated by a carrier or a carriage service provider; and

(ii) used in connection with the supply of a carriage service.

7 Section 5

Insert:

notifiable equipment has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

8 Section 5 (before paragraph (a) of the definition of *notification provision*)

Insert:

(aa) subsection 30EC(4); or

(ab) subsection 30EC(6); or

(ac) subsection 30ED(3); or

(ad) subsection 30ED(4); or

(ae) subsection 30EF(4); or

9 Section 5

Insert:

Outer Space Treaty means the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, done at London, Moscow and Washington on 27 January 1967, as amended and in force for Australia from time to time.

Note: The Treaty is in Australian Treaty Series 1967 No. 24 ([1967] ATS 24) and could in 2024 be viewed in the Australian Treaties Library on the AustLII website (http://www.austlii.edu.au).

satellite-based facility has the same meaning as in the *Telecommunications Act 1997*.

10 Section 5 (note to the definition of *space technology sector*)

Omit "Note", substitute "Note 1".

11 Section 5 (at the end of the definition of *space technology sector*)

Add:

Note 2: A critical telecommunications asset that is owned or operated by a carrier may be part of the space technology sector.

12 Section 5

Insert:

submarine cable has the same meaning as in Schedule 3A to the *Telecommunications Act 1997*.

telecommunications service has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

telecommunications system has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

13 Subsection 9(2B)

Omit "An asset", substitute "Subject to subsections (2C) and (2D), an asset".

14 After subsection 9(2B)

Insert:

(2C) Subsection (2B) does not apply for the purposes of working out whether a satellite-based facility is a critical telecommunications asset if the satellite-based facility is in a satellite to which either or both of the following apply:

(a) the satellite is included in the Register of Space Objects kept under section 76 of the *Space (Launches and Returns) Act 2018*;

(b) Australia is the appropriate State Party for the purposes of undertaking the authorisation and continuing supervision required in respect of the satellite under Article VI of the Outer Space Treaty.

Note: For the definitions of ***Outer Space Treaty*** and ***satellite-based facility***, see section 5.

(2D) Subsection (2B) does not apply for the purposes of working out whether a submarine cable is a critical telecommunications asset if the submarine cable is installed in Australian waters.

Note: For the definitions of ***submarine cable*** and ***Australian waters***, see section 5.

15 Subsection 10(1) (note)

Omit "Note", substitute "Note 1".

16 At the end of subsection 10(1)

Add:

Note 2: A critical electricity asset that is owned or operated by a carrier may also be a critical telecommunications asset.

17 Subsection 12B(1) (note)

Omit "Note", substitute "Note 1".

18 At the end of subsection 12B(1)

Add:

Note 2: A critical freight infrastructure asset that is owned or operated by a carrier may also be a critical telecommunications asset.

19 Subsection 12C(1) (note)

Omit "Note", substitute "Note 1".

20 At the end of subsection 12C(1)

Add:

Note 2: A critical freight services asset that is owned or operated by a carrier may also be a critical telecommunications asset.

21 Subsection 12F(1) (note)

Omit "Note", substitute "Note 1".

22 At the end of subsection 12F(1)

Add:

Note 2: A critical data storage or processing asset that is owned or operated by a carrier may also be a critical telecommunications asset.

23 Subsection 12F(2) (note)

Omit "Note", substitute "Note 1".

24 At the end of subsection 12F(2)

Add:

Note 2: A critical data storage or processing asset that is owned or operated by a carrier may also be a critical telecommunications asset.

25 After subparagraph 12N(3)(b)(iii)

Insert:

(iiia) under an authorisation given under section 31A of the *Telecommunications (Interception and Access) Act 1979*; or

26 After paragraph 30AG(2)(d)

Insert:

(da) if one or more of those assets are critical telecommunications assets:

(i) includes a summary of the changes (if any) the entity notified during the relevant period under subsection 30EC(2); and

(ii) describes the risks (if any) advised to the entity during the relevant period under paragraph 30ED(3)(c); and

(iii) describes the measures (if any) the entity adopted during the relevant period to eliminate or reduce risks advised to the entity during the relevant period or any previous period; and

(iv) includes a statement that evaluates the effectiveness of those measures to eliminate or reduce risks advised to the entity during the relevant period or any previous period; and

27 After Part 2C

Insert:

Part 2D—Enhanced security regulation for critical telecommunications assets

Division 1—Introduction

30EA Simplified outline of this Part

The responsible entity for a critical telecommunications asset that is prescribed by the rules has an obligation to protect the asset, so far as it is reasonably practicable to do so, for the purposes of:

(a) security; and

(b) the protection of the asset from any hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset.

The responsible entity for a critical telecommunications asset that is prescribed by the rules must notify the Secretary of certain changes, and proposed changes, to telecommunications services or telecommunications systems if the change, or proposed change, is likely to have a material adverse effect on the entity's capacity to comply with the obligation to protect the asset for the purposes of security.

The Minister may direct the responsible entity for a critical telecommunications asset not to use or supply, or to cease using or supplying, a carriage service, if the Minister considers that the use or supply would be, or is, prejudicial to security.

Division 2—Responsible entity's obligation to protect critical telecommunications assets

30EB Responsible entity's obligation to protect critical telecommunications assets

(1) This section applies to a critical telecommunications asset that is prescribed by the rules for the purposes of this subsection.

Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*.

(2) For the purposes of security and the protection of a critical telecommunications asset from any hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, the responsible entity for the asset must, so far as it is reasonably practicable to do so, protect the asset to ensure:

(a) the confidentiality of communications (as defined in the *Telecommunications Act 1997*) carried on, and of information contained on, the asset; and

(b) the availability and integrity of the asset.

Note: Security has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*: see the definition of ***security*** in section 5 of this Act.

Civil penalty: 1,500 penalty units.

(3) Without limiting subsection (2), the responsible entity's obligation under that subsection in respect of the critical telecommunications asset includes complying with the following:

(a) any requirements that apply to the entity and the asset under Part 2A (critical infrastructure risk management programs);

(b) the requirement to maintain competent supervision of, and effective control over, the asset;

(c) any other requirements prescribed by the rules for the purposes of this paragraph.

(4) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in performance of the obligation imposed by subsection (2).

(5) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (4).

Division 3—Responsible entity's notification obligations impacting their security obligations

30EC Responsible entity to notify certain changes and proposed changes to telecommunications service or system

(1) This section applies if, at any time, the responsible entity for a critical telecommunications asset prescribed by the rules for the purposes of this subsection becomes aware that the implementation of a change, or proposed change, by the entity to:

(a) a telecommunications service; or

(b) a telecommunications system;

is likely to have a material adverse effect on the entity's capacity to comply with its obligation under subsection 30EB(2), to the extent that subsection applies for the purposes of security and the asset.

Note 1: For specification by class, see subsection 13(3) of the *Legislation Act 2003*.

Note 2: See section 30EE for the kinds of changes covered by this Division.

(2) As soon as reasonably practicable after becoming aware that the change, or proposed change, is likely to have a material adverse effect as mentioned in subsection (1), the responsible entity for the critical telecommunications asset must:

(a) notify the Secretary, in writing, of the change, or of the entity's intention to implement the proposed change; and

(b) specify the asset in the notification; and

(c) include in the notification a description of the change or proposed change; and

(d) in relation to the change or proposed change—include in the notification any other information of a kind prescribed by the rules for the purposes of this paragraph.

Civil penalty: 300 penalty units.

(3) Information of a kind prescribed by the rules for the purposes of paragraph (2)(d) must be information that relates to changes, or proposed changes, to telecommunications services or telecommunications systems.

Further information

(4) If:

(a) the responsible entity for a critical telecommunications asset gives a notification under subsection (2) in relation to a change or proposed change; and

(b) the Secretary considers that further information is required for the Secretary to assess whether, in relation to the change or proposed change, there is a risk to the asset that would be prejudicial to security;

the Secretary may, by written notice given to the entity, require the entity to give the Secretary specified further information by the end of:

(c) 44 business days after the day the notice is given; or

(d) such longer period as the Secretary allows.

(5) The Secretary must give any notice under subsection (4) by the end of 22 business days after the day the Secretary receives the notification under subsection (2).

(6) If the Secretary:

(a) gives a notice to the entity under subsection (4) in relation to specified further information; and

(b) considers that information additional to the specified further information is required for the Secretary to make the assessment mentioned in paragraph (4)(b);

the Secretary may give the entity a further notice under subsection (4) in relation to the additional further information. Subsection (5) does not apply to the further notice.

Compliance with notice

(7) The responsible entity for a critical telecommunications asset must comply with a notice given to the entity under subsection (4).

Note: If the entity is not a legal person, see Division 2 of Part 7.

Civil penalty: 150 penalty units.

Self-incrimination

(8) An entity is not excused from giving information under subsection (7) on the ground that the information might tend to incriminate the entity or expose the entity to a penalty.

(9) However, in the case of an individual:

(a) the information given; or

(b) giving the information; or

(c) any information, document or thing obtained as a direct or indirect consequence of giving the information;

is not admissible in evidence against the individual:

(d) in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act; or

(e) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of subsection (7) of this section.

30ED Secretary to assess notified changes and proposed changes

(1) This section applies if, under subsection 30EC(2), the responsible entity for a critical telecommunications asset gives the Secretary a notification of a change or proposed change.

(2) The Secretary must give the entity a notice under subsection (3) or (4) of this section:

(a) by the end of 22 business days after the day the Secretary receives the notification, unless paragraph (b) of this subsection applies; or

(b) if the Secretary sought further information from the entity by one or more notices given under subsection 30EC(4)—as soon as practicable, and no later than 22 business days, after the day the entity provided the information sought by the last notice given under that subsection.

(3) If:

(a) the Secretary considers the change or proposed change (including where further information is provided in response to a notice given under subsection 30EC(4)); and

(b) in relation to the change or proposed change, the Secretary is satisfied that there is a risk to the asset that would be prejudicial to security;

the Secretary:

(c) must give a written notice to the entity:

(i) advising the entity of that risk; and

(ii) setting out the entity's obligation under subsection 30EB(2); and

(iii) setting out the consequences for the entity for not complying with that obligation; and

(d) may set out in that notice the measures the Secretary considers the entity could adopt to eliminate or reduce that risk.

(4) If:

(a) the Secretary considers the change or proposed change (including where further information is provided in response to a notice given under subsection 30EC(4)); and

(b) in relation to the change or proposed change, the Secretary is satisfied that there is not a risk to the asset that would be prejudicial to security;

the Secretary must give a written notice to the entity to that effect.

30EE Kinds of changes and proposed changes to telecommunications services or telecommunications systems

(1) For the purposes of this Division, a change or proposed change to a telecommunications service or a telecommunications system includes (but is not limited to) the following:

(a) the responsible entity concerned providing one or more new telecommunication services;

(b) the responsible entity concerned changing the location of notifiable equipment (including moving equipment outside Australia);

(c) the responsible entity concerned procuring notifiable equipment (including procuring equipment that is located outside Australia);

(d) the responsible entity concerned entering into outsourcing arrangements:
(i) to have all or part of the telecommunication services provided for that entity; or
(ii) to have all or part of the provision of telecommunication services managed for that entity; or
(iii) to have all or some information to which section 276 of the *Telecommunications Act 1997* applies in relation to that entity, managed for that entity;
(e) the responsible entity concerned entering into arrangements to have all or some information to which section 276 of the *Telecommunications Act 1997* applies in relation to that entity accessed by persons outside Australia;
(f) the responsible entity concerned entering into arrangements to have all or some information or documents to which subsection 187A(1) of the *Telecommunications (Interception and Access) Act 1979* applies in relation to that entity kept outside Australia.

(2) This Division does not apply to changes or proposed changes to a telecommunications service or a telecommunications system that are changes, or proposed changes, determined in an instrument under subsection (3).

(3) The Secretary may, by legislative instrument, make a determination for the purposes of subsection (2).

Division 4—Ministerial directions

30EF Minister's direction if use or supply of carriage services prejudicial to security

(1) If:
(a) the responsible entity for a critical telecommunications asset proposes to use, or uses, for the entity's own requirements or benefit, or proposes to supply, or supplies, to another person, one or more carriage services; and
(b) the Minister considers that the proposed use or supply would be, or the use or supply is, as the case may be, prejudicial to security;

the Minister may give the entity a written direction not to use or supply, or to cease using or supplying, the carriage service or the carriage services.

(2) A direction under subsection (1) must:
  (a) relate to a carriage service generally and cannot be expressed to apply to the supply of a carriage service to a particular person, particular persons or a particular class of persons; and
  (b) specify the period within which the entity must comply with the direction (which must be a period that is reasonable in the circumstances).

Direction to be given after adverse security assessment

(3) The Minister must not give the responsible entity for a critical telecommunications asset a direction under subsection (1) unless an adverse security assessment in respect of the carrier or carriage service provider is given to the Minister in connection with this section.

Copy of direction to be given to ACMA

(4) The Minister must give the Australian Communications and Media Authority a copy of any direction under subsection (1).

Compliance with direction

(5) The responsible entity for a critical telecommunications asset must comply with a direction given to the entity under subsection (1).

Civil penalty: 2,000 penalty units.

Liability

(6) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction under subsection (1).

(7) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (6).

Interaction with section 32

(8) This section does not limit section 32 (direction if risk of act or omission that would be prejudicial to security).

28 After paragraph 60(2)(a)

Insert:

(aa) the number of notifications that were made during the financial year to the Secretary under Division 3 of Part 2D (responsible entity's notification obligations impacting their security obligations); and

(ab) any directions given during the financial year by the Minister under section 30EF (Minister's direction if use or supply of carriage services prejudicial to security); and

Part 2—Consequential amendments

Australian Security Intelligence Organisation Act 1979

29 Subsection 35(1) (subparagraph (d)(ii) of the definition of *prescribed administrative action*)

Repeal the subparagraph.

30 Subsection 35(1) (paragraph (e) of the definition of *prescribed administrative action*)

After "subsection", insert "30EF(1) or".

Telecommunications Act 1997

34 Section 5

Omit:

> • The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.
>
> • Carriers and carriage service providers must do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access.

substitute:

> • The ACMA, carriers and carriage service providers must prevent, so far as it is reasonably practicable to do so, telecommunications networks and facilities from being used to commit offences.

35 Section 311

Omit:

- The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.
- Carriers and carriage service providers have a duty to do their best to protect telecommunications networks and facilities from unauthorised interference, or unauthorised access, for the purposes of security. Carriers and certain carriage service providers must notify changes to telecommunications services or telecommunications systems that are likely to have a material adverse effect on their capacity to comply with this duty.

substitute:

- The ACMA, carriers and carriage service providers must prevent, so far as it is reasonably practicable to do so, telecommunications networks and facilities from being used to commit offences.

36 Section 311

Omit:

- The Home Affairs Minister may give directions to a carrier or a carriage service provider in certain circumstances where certain activities may be prejudicial to security.
- The Home Affairs Secretary may obtain information from carriers, carriage service providers and carriage service intermediaries if the information is relevant to assessing compliance with the duty of those persons to protect telecommunications networks and facilities from unauthorised interference or unauthorised access.

37 Subsection 312(1)

Omit "do its best to prevent", substitute "prevent, so far as it is reasonably practicable to do so".

38 Subsection 313(1)

Omit "do the carrier's best or the provider's best to prevent", substitute "prevent, so far as it is reasonably practicable to do so,".

39 Subsections 313(1A) and (1B)

Repeal the subsections.

40 Subsection 313(2)

Omit "do the intermediary's best to prevent", substitute "prevent, so far as it is reasonably practicable to do so,".

41 Subsection 313(2A)

Repeal the subsection.

42 Paragraph 313(5)(a)

Omit "(1A),".

43 Paragraph 313(5)(a)

Omit "(2A),".

44 Paragraph 313(5)(b)

Omit "312; or", substitute "312.".

45 Paragraph 313(5)(c)

Repeal the paragraph.

46 Divisions 3, 5, 6, 7, 8 and 8A of Part 14

Repeal the Divisions.

47 Subsections 564(1) and (2)

Omit ", the ACCC or the Home Affairs Minister", substitute "or the ACCC".

48 Subsection 564(3A)

Repeal the subsection.

49 Subsection 571(1)

Omit ", the ACCC or the Home Affairs Minister", substitute "or the ACCC".

50 Subsection 571(4)

Repeal the subsection.

51 Section 572A

Omit "or the Home Affairs Minister".

52 Subsection 572B(1), (3) and (4)

Omit "or the Home Affairs Minister".

53 Subsection 572B(5)

Omit "The Home Affairs Minister may arrange for the publishing of the undertaking on the Home Affairs Department's website.".

54 Subsection 572B(5A)

Repeal the subsection.

55 Subsection 572B(5B)

Omit "The Home Affairs Minister's powers under those subsections are only in relation to undertakings he or she has accepted.".

56 Subsection 572C(1)

Omit "or the Home Affairs Minister" (wherever occurring).

57 Subsection 572C(3)

Omit "The Home Affairs Minister's power under that subsection is only in relation to undertakings he or she has accepted.".

Telecommunications (Interception and Access) Act 1979

58 Subparagraph 202A(a)(ii)

Omit "(other than subsection 313(1A) or (2A) of that Act)".

59 Paragraph 202B(1)(b)

Omit "(other than subsection 313(1A) or (2A) of that Act)".

Part 3—Contingent amendments

Division 1—Amendments contingent on the commencement of Schedule 3 to this Act

Security of Critical Infrastructure Act 2018

60 After paragraph 5A(3)(l)

Insert:

(la) records or is the fact that the Minister has:

(i) given a direction under subsection 30EF(1); or

(ii) revoked such a direction; or

Division 2—Amendments if Schedule 4 to the Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2024 commences before Part 2 of this Schedule

Telecommunications Act 1997

61 Section 7 (definition of *Communications Security Coordinator*)

Repeal the definition.

62 Section 7A

Repeal the section.

Division 3—Amendments if Schedule 4 to the Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2024 does not commence before Part 2 of this Schedule

Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2024

63 Items 2, 3 and 15 to 48 of Schedule 4

Repeal the items.

64 Item 162 of Schedule 4

Omit "or a Communications Security Coordinator".

65 Items 164 to 167 of Schedule 4

Repeal the items.

Part 4—Application and saving provisions

66 Application provisions—*Security of Critical Infrastructure Act 2018*

(1) To avoid doubt, the amendment of the definition of ***critical telecommunications asset*** in section 5 of the *Security of Critical Infrastructure Act 2018* made by Part 1 of this Schedule does not affect the following:

(a) the continuity of a declaration under section 52B of that Act that:

(i) relates to an asset that is covered by the definition of ***critical telecommunications asset*** as amended; and

(ii) is in force immediately before the day this item commences;

(b) the operation of Part 2C of that Act in relation to the asset mentioned in subparagraph (a)(i) of this subitem.

(2) The amendment of subsection 12N(3) of the *Security of Critical Infrastructure Act 2018* made by Part 1 of this Schedule applies in relation to the causing of any access, modification or impairment of a kind mentioned in subsection 12N(1) of that Act on or after the day this item commences.

(3) The amendment of section 30AG of the *Security of Critical Infrastructure Act 2018* made by Part 1 of this Schedule applies in relation to a financial year that ends after the day this item commences.

(4) Section 30EB of the *Security of Critical Infrastructure Act 2018*, as inserted by Part 1 of this Schedule, applies in relation to the protection of a critical telecommunications asset in respect of days occurring on or after the day this item commences.

(5) Section 30EC of the *Security of Critical Infrastructure Act 2018*, as inserted by Part 1 of this Schedule, applies in relation to a change or proposed change if the responsible entity for a critical telecommunications asset first becomes aware of the likely effect of the change or proposed change on or after the day this item commences, regardless of when the change was implemented or proposed.

(6) Section 30EF of the *Security of Critical Infrastructure Act 2018*, as inserted by Part 1 of this Schedule, applies in relation to the use or supply of a carriage service on or after the day this item commences, regardless of when the use or supply starts.

(7) The amendment of section 60 of the *Security of Critical Infrastructure Act 2018* made by Part 1 of this Schedule applies in relation to a financial year that ends after the day this item commences.

67 Saving provision—*Australian Security Intelligence Organisation Act 1979*

Despite the amendments of section 35 of the *Australian Security Intelligence Organisation Act 1979* made by Part 2 of this Schedule, Part IV of that Act, as in force immediately before the day this item commences, continues to apply on and after that day in connection with the giving of a direction under subsection 315A(1) or 315B(2) of the *Telecommunications Act 1997* before that day.

68 Application and saving provisions—*Telecommunications Act 1997*

(1) The amendment of subsection 312(1) of the *Telecommunications Act 1997* made by Part 2 of this Schedule applies in relation to working out whether ACMA has complied with the duty imposed by that subsection in relation to days occurring on or after the day this item commences.

(2) The amendment of subsection 313(1) of the *Telecommunications Act 1997* made by Part 2 of this Schedule applies in relation to working out whether a carrier or carriage service provider has complied with the duty imposed by that subsection in relation to days occurring on or after the day this item commences.

(3) Despite the repeal of subsections 313(1A) and (1B) of the *Telecommunications Act 1997* by Part 2 of this Schedule, those subsections and other provisions of that Act that relate to those subsections, as in force immediately before the day this item commences, continue to apply on and after that day in relation to the protection of telecommunications networks and facilities in respect of days occurring before the day this item commences.

(4) The amendment of subsection 313(2) of the *Telecommunications Act 1997* made by Part 2 of this Schedule applies in relation to working out

whether a carrier service intermediary has complied with the duty imposed by that subsection in relation to days occurring on or after the day this item commences.

(5) Despite the repeal of subsection 313(2A) of the *Telecommunications Act 1997* by Part 2 of this Schedule, that subsection and other provisions of that Act that relate to that subsection, as in force immediately before the day this item commences, continue to apply on and after that day in relation to the protection of telecommunications networks and facilities in respect of days occurring before the day this item commences.

(6) Despite the amendments of subsection 313(5) of the *Telecommunications Act 1997* made by Part 2 of this Schedule, that subsection, as in force immediately before the day this item commences, continues to apply on and after that day in relation to the following:

(a) an act done or omitted in good faith before that day in the performance of the duty imposed by subsection 313(1A) or (2A) of that Act before that day;

(b) an act done or omitted in good faith before, on or after that day in compliance with a direction given under subsection 315A(1) or 315B(2) of that Act before that day.

(7) Despite the repeal of sections 314A and 314B of the *Telecommunications Act 1997* made by Part 2 of this Schedule, those sections and other provisions of that Act that relate to those sections, as in force immediately before the day this item commences, continue to apply on and after that day in relation to a proposed change if a carrier or a nominated carriage service provider first becomes aware of the likely effect of the proposed change before that day.

(8) Despite the repeal of section 315A of the *Telecommunications Act 1997* by Part 2 of this Schedule, that section and other provisions of that Act that relate to that section, as in force immediately before the day this item commences, continue to apply on and after that day in relation to a direction given under subsection 315A(1) of that Act before that day.

(9) An adverse security assessment that is given, before the day this item commences, to the Home Affairs Minister in connection with section 315A of the *Telecommunications Act 1997* has effect, on and after that day, as if it were also given in connection with section 30EF

of the *Security of Critical Infrastructure Act 2018*, as inserted by Part 1 of this Schedule.

(10) Despite the repeal of section 315B of the *Telecommunications Act 1997* by Part 2 of this Schedule, that section and other provisions of that Act that relate to that section, as in force immediately before the day this item commences, continue to apply on and after that day in relation to a direction given under subsection 315B(2) of that Act before that day.

(11) Despite the repeal of Division 6 of Part 14 of the *Telecommunications Act 1997* by Part 2 of this Schedule, that Division and other provisions of that Act that relate to that Division, as in force immediately before the day this item commences, continue to apply on and after that day in relation to a notice given under subsection 315C(2) of that Act before that day.

(12) Despite the repeal of section 315H of the *Telecommunications Act 1997* by Part 2 of this Schedule, that section and other provisions of that Act that relate to that section, as in force immediately before the day this item commences, continue to apply on and after that day in relation to the disclosure of information, or the provision of a document, on or after that day, regardless of when the information or document was obtained.

(13) Despite the repeal of section 315J of the *Telecommunications Act 1997* by Part 2 of this Schedule, that section, as in force immediately before the day this item commences, continues to apply on and after that day in relation to a financial year that commenced before that day.

(14) Despite the amendments of section 564 of the *Telecommunications Act 1997* made by Part 2 of this Schedule, that section, as in force immediately before the day this item commences, continues to apply on and after that day in relation to the following:

(a) an application made by the Home Affairs Minister before that day;

(b) the making of an application by the Home Affairs Minister on or after that day.

(15) Despite the amendments of section 571 of the *Telecommunications Act 1997* made by Part 2 of this Schedule, that section, as in force immediately before the day this item commences, continues to apply on and after that day in relation to the following:

(a) a proceeding instituted by the Home Affairs Minister before that day;
(b) the institution of a proceeding by the Home Affairs Minister on or after that day.

(16) Despite the amendments of section 572B of the *Telecommunications Act 1997* made by Part 2 of this Schedule, that section, as in force immediately before the day this item commences, continues to apply on and after that day in relation to an undertaking given to the Home Affairs Minister before, on or after that day.

(17) Despite the amendments of section 572C of the *Telecommunications Act 1997* made by Part 2 of this Schedule, that section, as in force immediately before the day this item commences, continues to apply on and after that day in relation to an undertaking accepted by the Home Affairs Minister before, on or after that day.

69 Saving provision—*Telecommunications (Interception and Access) Act 1979*

Despite the amendments of sections 202A and 202B of the *Telecommunications (Interception and Access) Act 1979* made by Part 2 of this Schedule, those sections, as in force immediately before the day this item commences, continue to apply on and after that day in relation to a proposed change if a carrier or nominated carriage service provider first becomes aware of the likely effect of the proposed change before the day this item commences.

70 Transitional rules

(1) The Minister may, by legislative instrument, make rules prescribing matters of a transitional nature (including prescribing any saving or application provisions) relating to the amendments or repeals made by this Schedule.

(2) To avoid doubt, the rules may not do the following:
(a) create an offence or civil penalty;
(b) provide powers of:
(i) arrest or detention; or
(ii) entry, search or seizure;
(c) impose a tax;

(d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;

(e) directly amend the text of this Schedule.

(3) This Part (other than subitem (2)) does not limit the rules that may be made for the purposes of subitem (1).

Schedule 6—Notification of declaration of system of national significance

Security of Critical Infrastructure Act 2018

1 Section 5 (paragraphs (r) and (s) of the definition of *notification provision*)

Repeal the paragraphs, substitute:

(r) subsection 52B(3).

2 Section 52A

Omit "each reporting entity for an asset that is a declared system of national significance", substitute "the responsible entity for an asset that is a declared system of national significance of the declaration".

3 Section 52A

Omit:

> If a reporting entity for an asset that is a declared system of national significance ceases to be such a reporting entity, or becomes aware of another reporting entity for the asset, the entity must notify the Secretary.

substitute:

> If the responsible entity for an asset that is a declared system of national significance ceases to be the responsible entity for the asset, the entity must notify the Secretary.

4 Paragraph 52B(3)(a)

Repeal the paragraph, substitute:

(a) the responsible entity for the asset;

5 Section 52D

Repeal the section, substitute:

52D Notification if responsible entity for an asset ceases to be the responsible entity

If the responsible entity for an asset declared under subsection 52B(1) to be a system of national significance ceases to be the responsible entity for the asset, the entity must, within 30 days, notify the Secretary of that cessation.

Civil penalty: 150 penalty units.

6 Application and saving provisions

(1) The amendment of section 52B of the *Security of Critical Infrastructure Act 2018* made by this Schedule applies in relation to a declaration made under subsection 52B(1) of that Act on or after the day on which this item commences.

(2) Section 52D of the *Security of Critical Infrastructure Act 2018*, as substituted by this Schedule, applies in relation to a cessation that occurs on or after the day on which this item commences.

(3) The *Security of Critical Infrastructure Act 2018*, as in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to a matter referred to in paragraph 52D(1)(a) or (b) of that Act that occurred before that commencement.

Schedule 7—Notification of certain critical infrastructure or telecommunications security assessments

Australian Security Intelligence Organisation Act 1979

1 Subsection 38(1A)

Repeal the subsection.

2 Section 38A

Repeal the section.

3 Subsection 54(2)

Omit "or 38A".

4 Application provision—repeal of section 38A of the *Australian Security Intelligence Organisation Act 1979*

The amendments of Part IV of the *Australian Security Intelligence Organisation Act 1979* made by this Schedule apply in relation to a security assessment in respect of a person that is furnished by the Organisation on or after the commencement of this Schedule.

5 Application provision—confirmation of application of section 38 of the *Australian Security Intelligence Organisation Act 1979* to certain critical infrastructure or telecommunications assessments

(1) The object of this item is to confirm the application of section 38 of the *Australian Security Intelligence Organisation Act 1979* in relation to an adverse or qualified security assessment (a ***relevant assessment***) that was furnished:

(a) by the Organisation:

(i) in connection with section 58A, 315A or 315B of, or clause 57A or 72A of Schedule 3A to, the *Telecommunications Act 1997*; or

(ii) for the purposes of section 32 of the *Security of Critical Infrastructure Act 2018*; and

(b) at a time before the commencement of this Schedule; and

(c) to a Minister who, at that time, was not the ASIO Minister.

(2) A notice given, or purportedly given, by a Commonwealth agency for the purposes of subsection 38(1) of the *Australian Security Intelligence Organisation Act 1979* in relation to a relevant assessment is taken for all purposes to have been, and to always have been, given under that subsection.

(3) A certificate issued, or purportedly issued, by the ASIO Minister for the purposes of subsection 38(2) of the *Australian Security Intelligence Organisation Act 1979* in relation to a relevant assessment is taken for all purposes to have been, and to always have been, issued under that subsection.

(4) To avoid doubt, anything done, or anything purported to have been done, by a person that would have been wholly or partly invalid except for subitem (2) or (3) is taken for all purposes to be valid and to have always been valid, despite any effect that may have on the accrued rights of any person.

(5) For the purposes of applying this item in relation to civil or criminal proceedings, this item applies in relation to:

(a) civil and criminal proceedings instituted on or after the commencement of this Schedule; and

(b) civil and criminal proceedings instituted before commencement, being proceedings that are concluded:

(i) before the commencement of this Schedule; or

(ii) on or after the commencement of this Schedule.

(6) In this item:

ASIO Minister means the Minister administering Part II of the *Australian Security Intelligence Organisation Act 1979*.

do a thing includes:

(a) make a decision (however described); and

(b) exercise a power, perform a function, comply with an obligation or discharge a duty; and

(c) do anything else;

and ***purport to do a thing*** has a corresponding meaning.

Schedule 8—Other amendments

Security of Critical Infrastructure Act 2018

1 Section 60AAA

Repeal the section.

2 Section 60B

Omit "3 years", substitute "5 years".

[*Minister's second reading speech made in—*
House of Representatives on 9 October 2024
Senate on 25 November 2024]

(121/24)