# Security Legislation Amendment (Critical Infrastructure) Act 2021

# No. 124, 2021

## An Act to amend legislation relating to critical infrastructure, and for other purposes

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

# Contents


1 Short title ..... 1
2 Commencement ..... 2
3 Schedules ..... 3

**Schedule 1—Security of critical infrastructure** 4

Part 1—General amendments 4

*Administrative Decisions (Judicial Review) Act 1977* 4

*Security of Critical Infrastructure Act 2018* 4

Part 2—Application provisions 104

Part 3—Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2021 105

*Security of Critical Infrastructure Act 2018* 105

Part 4—Amendments contingent on the commencement of the National Emergency Declaration Act 2020 106

*National Emergency Declaration Act 2020* 106

*Security of Critical Infrastructure Act 2018* 106

**Schedule 2—Australian Signals Directorate** 107

*Criminal Code Act 1995* 107

# Security Legislation Amendment (Critical Infrastructure) Act 2021

**No. 124, 2021**

## An Act to amend legislation relating to critical infrastructure, and for other purposes

[*Assented to 2 December 2021*]

The Parliament of Australia enacts:

### 1 Short title

This Act is the *Security Legislation Amendment (Critical Infrastructure) Act 2021*.

## 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. | 2 December 2021 |
| 2. Schedule 1, Parts 1 and 2 | The day after this Act receives the Royal Assent. | 3 December 2021 |
| 3. Schedule 1, Part 3 | The later of:<br>(a) immediately after the commencement of the provisions covered by table item 2; and<br>(b) the commencement of the *Federal Circuit and Family Court of Australia Act 2021*.<br>However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur. | 3 December 2021<br>(paragraph (a) applies) |
| 4. Schedule 1, Part 4 | The later of:<br>(a) immediately after the commencement of the provisions covered by table item 2; and<br>(b) the commencement of the *National Emergency Declaration Act 2020*.<br>However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur. | 3 December 2021<br>(paragraph (a) applies) |
| 5. Schedule 2 | The day after this Act receives the Royal Assent. | 3 December 2021 |

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—Security of critical infrastructure

## Part 1—General amendments

### *Administrative Decisions (Judicial Review) Act 1977*

#### 1 Before paragraph (da) of Schedule 1

Insert:

(dae) decisions under Part 3A of the *Security of Critical Infrastructure Act 2018*;

### *Security of Critical Infrastructure Act 2018*

#### 4 Section 3

Omit "to national security".

#### 5 At the end of section 3

Add:

; and (e) providing a regime for the Commonwealth to respond to serious cyber security incidents.

#### 6 Section 4

Repeal the section, substitute:

**4 Simplified outline of this Act**

This Act creates a framework for managing risks relating to critical infrastructure.

The framework consists of the following:

(a) the keeping of a register of information in relation to critical infrastructure assets (the register will not be made public);

(c) requiring notification of cyber security incidents;

(e) requiring certain entities relating to a critical infrastructure asset to provide information in relation to

the asset, and to notify if certain events occur in relation to the asset;

(f) allowing the Minister to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security;

(g) allowing the Secretary to require certain entities relating to a critical infrastructure asset to provide certain information or documents;

(h) setting up a regime for the Commonwealth to respond to serious cyber security incidents;

(i) allowing the Secretary to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset.

Certain information obtained or generated under, or relating to the operation of, this Act is protected information. There are restrictions on when a person may make a record of, use or disclose protected information.

Civil penalty provisions of this Act may be enforced using civil penalty orders, injunctions or infringement notices, and enforceable undertakings may be accepted in relation to compliance with civil penalty provisions. The Regulatory Powers Act is applied for these purposes. Certain provisions of this Act are subject to monitoring and investigation under the Regulatory Powers Act. Certain provisions of this Act may be enforced by imposing a criminal penalty.

The Minister may privately declare an asset to be a critical infrastructure asset.

The Secretary must give the Minister reports, for presentation to the Parliament, on the operation of this Act.

## 7 Section 5

Insert:

***access***, in relation to a computer program, means the execution of the computer program.

***access to computer data*** means:

(a) in a case where the computer data is held in a computer—the display of the data by the computer or any other output of the data from the computer; or

(b) in a case where the computer data is held in a computer—the copying or moving of the data to:

(i) any other location in the computer; or

(ii) another computer; or

(iii) a data storage device; or

(c) in a case where the computer data is held in a data storage device—the copying or moving of the data to:

(i) a computer; or

(ii) another data storage device.

***aircraft operator*** has the same meaning as in the *Aviation Transport Security Act 2004*.

***airport*** has the same meaning as in the *Aviation Transport Security Act 2004*.

***airport operator*** has the same meaning as in the *Aviation Transport Security Act 2004*.

***air service*** has the same meaning as in the *Aviation Transport Security Act 2004*.

***approved staff member of the authorised agency*** has the meaning given by section 35BJ.

***ASD*** means the Australian Signals Directorate.

***asset*** includes:

(a) a system; and

(b) a network; and

(c) a facility; and

(d) a computer; and

(e) a computer device; and

(f) a computer program; and

(g) computer data; and
(h) premises; and
(i) any other thing.

***associated entity*** has the same meaning as in the *Corporations Act 2001*.

***associated transmission facility*** means:
(a) an antenna; or
(b) a combiner; or
(c) a feeder system; or
(d) an apparatus; or
(e) an item of equipment; or
(f) a structure; or
(g) a line; or
(h) an electricity cable or wire;
that is associated with a radiocommunications transmitter.

***AusCheck scheme*** has the same meaning as in the *AusCheck Act 2007*.

***Australia***, when used in a geographical sense, includes the external Territories.

***Australian CS facility licence*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***Australian derivative trade repository licence*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***Australian market licence*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***authorised agency*** means ASD.

***authorised deposit-taking institution*** has the same meaning as in the *Banking Act 1959*.

***background check*** has the same meaning as in the *AusCheck Act 2007*.

***banking business*** has the same meaning as in the *Banking Act 1959*.

***benchmark administrator licence*** has the same meaning as in the *Corporations Act 2001*.

***broadcasting re-transmission asset*** means:

(a) a radiocommunications transmitter; or

(b) a broadcasting transmission tower; or

(c) an associated transmission facility;

that is used in connection with the transmission of a service to which, as a result of section 212 of the *Broadcasting Services Act 1992*, the regulatory regime established by that Act does not apply.

***broadcasting service*** has the same meaning as in the *Broadcasting Services Act 1992*.

***broadcasting transmission asset*** means:

(a) a radiocommunications transmitter; or

(b) a broadcasting transmission tower; or

(c) an associated transmission facility;

that is used, or is capable of being used, in connection with the transmission of:

(d) a national broadcasting service; or

(e) a commercial radio broadcasting service; or

(f) a commercial television broadcasting service.

***broadcasting transmission tower*** has the same meaning as in Schedule 4 to the *Broadcasting Services Act 1992*.

***business critical data*** means:

(a) personal information (within the meaning of the *Privacy Act 1988*) that relates to at least 20,000 individuals; or

(b) information relating to any research and development in relation to a critical infrastructure asset; or

(c) information relating to any systems needed to operate a critical infrastructure asset; or

(d) information needed to operate a critical infrastructure asset; or

(e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

***carriage service*** has the same meaning as in the *Telecommunications Act 1997*.

***carriage service provider*** has the same meaning as in the *Telecommunications Act 1997*.

***carrier*** has the same meaning as in the *Telecommunications Act 1997*.

***chief executive of the authorised agency*** means the Director-General of ASD.

***clearing and settlement facility*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***commercial radio broadcasting service*** has the same meaning as in the *Broadcasting Services Act 1992*.

***commercial television broadcasting service*** has the same meaning as in the *Broadcasting Services Act 1992*.

***communications sector*** means the sector of the Australian economy that involves:

(a) supplying a carriage service; or
(b) providing a broadcasting service; or
(c) owning or operating assets that are used in connection with the supply of a carriage service; or
(d) owning or operating assets that are used in connection with the transmission of a broadcasting service; or
(e) administering an Australian domain name system.

***computer*** means all or part of:

(a) one or more computers; or
(b) one or more computer systems; or
(c) one or more computer networks; or
(d) any combination of the above.

***computer data*** means data held in:

(a) a computer; or
(b) a data storage device.

***computer device*** means a device connected to a computer.

***connected*** includes connection otherwise than by means of physical contact, for example, a connection by means of radiocommunication.

***constable*** has the same meaning as in the *Crimes Act 1914*.

***credit facility*** has the meaning given by regulations made for the purposes of paragraph 12BAA(7)(k) of the *Australian Securities and Investments Commission Act 2001*.

***credit facility business*** means a business that offers, or provides services in relation to, a credit facility.

***critical aviation asset*** means:

(a) an asset that:
  (i) is used in connection with the provision of an air service; and
  (ii) is owned or operated by an aircraft operator; or
(b) an asset that:
  (i) is used in connection with the provision of an air service; and
  (ii) is owned or operated by a regulated air cargo agent; or
(c) an asset that is used by an airport operator in connection with the operation of an airport.

Note: The rules may prescribe that a specified critical aviation asset is not a critical infrastructure asset (see section 9).

***critical banking asset*** has the meaning given by section 12G.

Note: The rules may prescribe that a specified critical banking asset is not a critical infrastructure asset (see section 9).

***critical broadcasting asset*** has the meaning given by section 12E.

Note: The rules may prescribe that a specified critical broadcasting asset is not a critical infrastructure asset (see section 9).

***critical data storage or processing asset*** has the meaning given by section 12F.

Note: The rules may prescribe that a specified critical data storage or processing asset is not a critical infrastructure asset (see section 9).

***critical defence capability*** includes:

(a) materiel; and
(b) technology; and
(c) a platform; and
(d) a network; and
(e) a system; and
(f) a service;

that is required in connection with:

(g) the defence of Australia; or
(h) national security.

***critical defence industry asset*** means an asset that:

(a) is being, or will be, supplied by an entity to the Defence Department, or the Australian Defence Force, under a contract; and
(b) consists of, or enables, a critical defence capability.

Note: The rules may prescribe that a specified critical defence industry asset is not a critical infrastructure asset (see section 9).

***critical domain name system*** has the meaning given by section 12KA.

Note: The rules may prescribe that a specified critical domain name system is not a critical infrastructure asset (see section 9).

***critical education asset*** means a university that is owned or operated by an entity that is registered in the Australian university category of the National Register of Higher Education Providers.

Note: The rules may prescribe that a specified critical education asset is not a critical infrastructure asset (see section 9).

***critical energy market operator asset*** means an asset that:

(a) is owned or operated by:
(i) Australian Energy Market Operator Limited (ACN 072 010 327); or
(ii) Power and Water Corporation; or
(iii) Regional Power Corporation; or
(iv) Electricity Networks Corporation; and

(b) is used in connection with the operation of an energy market or system; and

(c) is critical to ensuring the security and reliability of an energy market;

but does not include:

(d) a critical electricity asset; or

(e) a critical gas asset; or

(f) a critical liquid fuel asset.

Note: The rules may prescribe that a specified critical energy market operator asset is not a critical infrastructure asset (see section 9).

***critical financial market infrastructure asset*** has the meaning given by section 12D.

Note: The rules may prescribe that a specified critical financial market infrastructure asset is not a critical infrastructure asset (see section 9).

***critical food and grocery asset*** has the meaning given by section 12K.

Note: The rules may prescribe that a specified critical food and grocery asset is not a critical infrastructure asset (see section 9).

***critical freight infrastructure asset*** has the meaning given by section 12B.

Note: The rules may prescribe that a specified critical freight infrastructure asset is not a critical infrastructure asset (see section 9).

***critical freight services asset*** has the meaning given by section 12C.

Note: The rules may prescribe that a specified critical freight services asset is not a critical infrastructure asset (see section 9).

***critical hospital*** means a hospital that has a general intensive care unit.

Note: The rules may prescribe that a specified critical hospital is not a critical infrastructure asset (see section 9).

***critical infrastructure sector*** has the meaning given by section 8D.

***critical infrastructure sector asset*** has the meaning given by subsection 8E(1).

***critical insurance asset*** has the meaning given by section 12H.

Note: The rules may prescribe that a specified critical insurance asset is not a critical infrastructure asset (see section 9).

***critical liquid fuel asset*** has the meaning given by section 12A.

Note: The rules may prescribe that a specified critical liquid fuel asset is not a critical infrastructure asset (see section 9).

***critical public transport asset*** means a public transport network or system that:

(a) is managed by a single entity; and

(b) is capable of handling at least 5 million passenger journeys per month;

but does not include a critical aviation asset.

Note: The rules may prescribe that a specified critical public transport asset is not a critical infrastructure asset (see section 9).

***critical superannuation asset*** has the meaning given by section 12J.

Note: The rules may prescribe that a specified critical superannuation asset is not a critical infrastructure asset (see section 9).

***critical telecommunications asset*** means:

(a) a telecommunications network that is:

(i) owned or operated by a carrier; and

(ii) used to supply a carriage service; or

(b) a telecommunications network, or any other asset, that is:

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

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

Note: The rules may prescribe that a specified critical telecommunications asset is not a critical infrastructure asset (see section 9).

***cyber security incident*** has the meaning given by section 12M.

***data*** includes information in any form.

***data storage*** means data storage that involves information technology, and includes data back-up.

***data storage device*** means a thing (for example, a disk or file server) containing (whether temporarily or permanently), or designed to contain (whether temporarily or permanently), data for use by a computer.

***data storage or processing provider*** means an entity that provides a data storage or processing service.

***data storage or processing sector*** means the sector of the Australian economy that involves providing data storage or processing services.

***data storage or processing service*** means:

(a) a service that enables end-users to store or back-up data; or

(b) a data processing service.

***Defence Department*** means the Department of State that deals with defence and that is administered by the Defence Minister.

***defence industry sector*** means the sector of the Australian economy that involves the provision of critical defence capabilities.

***Defence Minister*** means the Minister administering section 1 of the *Defence Act 1903*.

***derivative trade repository*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***Electricity Networks Corporation*** means the Electricity Networks Corporation established by section 4 of the *Electricity Corporations Act 2005* (WA).

***electronic communication*** means a communication of information in any form by means of guided or unguided electromagnetic energy.

***energy sector*** means the sector of the Australian economy that involves:

(a) the production, transmission, distribution or supply of electricity; or

(b) the production, processing, transmission, distribution or supply of gas; or

(c) the production, processing, transmission, distribution or supply of liquid fuel.

***engage in conduct*** means:

(a) do an act or thing; or

(b) omit to perform an act or thing.

***financial benchmark*** has the same meaning as in Part 7.5B of the *Corporations Act 2001*.

***financial market*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***financial services and markets sector*** means the sector of the Australian economy that involves:

(a) carrying on banking business; or
(b) operating a superannuation fund; or
(c) carrying on insurance business; or
(d) carrying on life insurance business; or
(e) carrying on health insurance business; or
(f) operating a financial market; or
(g) operating a clearing and settlement facility;
(h) operating a derivative trade repository; or
(i) administering a financial benchmark; or
(j) operating a payment system; or
(k) carrying on financial services business; or
(l) carrying on credit facility business.

***financial services business*** has the same meaning as in Chapter 7 of the *Corporations Act 2001*.

***food*** means food for human consumption.

***food and grocery sector*** means the sector of the Australian economy that involves:

(a) manufacturing; or
(b) processing; or
(c) packaging; or
(d) distributing; or
(e) supplying;

food or groceries on a commercial basis.

***gas*** means a substance that:

(a) is in a gaseous state at standard temperature and pressure; and

(b) consists of naturally occurring hydrocarbons, or a naturally occurring mixture of hydrocarbons and non-hydrocarbons, the principal constituent of which is methane; and

(c) is suitable for consumption.

***general intensive care unit*** means an area within a hospital that:

(a) is equipped and staffed so that it is capable of providing to a patient:

(i) mechanical ventilation for a period of several days; and

(ii) invasive cardiovascular monitoring; and

(b) is supported by:

(i) during normal working hours—at least one specialist, or consultant physician, in the specialty of intensive care, who is immediately available, and exclusively rostered, to that area; and

(ii) at all times—at least one medical practitioner who is present in the hospital and immediately available to that area; and

(iii) at least 18 hours each day—at least one nurse; and

(c) has admission and discharge policies in operation.

***government business enterprise*** has the same meaning as in the *Public Governance, Performance and Accountability Act 2013*.

***health care*** includes:

(a) services provided by individuals who practise in any of the following professions or occupations:

(i) dental (including the profession of a dentist, dental therapist, dental hygienist, dental prosthetist and oral health therapist);

(ii) medical;

(iii) medical radiation practice;

(iv) nursing;

(v) midwifery;

(vi) occupational therapy;

(vii) optometry;

(viii) pharmacy;

(ix) physiotherapy;

(x) podiatry;
(xi) psychology;
(xii) a profession or occupation specified in the rules; and

(b) treatment and maintenance as a patient at a hospital.

***health care and medical sector*** means the sector of the Australian economy that involves:

(a) the provision of health care; or
(b) the production, distribution or supply of medical supplies.

***health insurance business*** has the same meaning as in the *Private Health Insurance Act 2007*.

***higher education and research sector*** means the sector of the Australian economy that involves:

(a) being a higher education provider; or
(b) undertaking a program of research that:
(i) is supported financially (in whole or in part) by the Commonwealth; or
(ii) is relevant to a critical infrastructure sector (other than the higher education and research sector).

***higher education provider*** has the same meaning as in the *Tertiary Education Quality and Standards Agency Act 2011*.

***hospital*** has the same meaning as in the *Private Health Insurance Act 2007*.

***IGIS official*** means:

(a) the Inspector-General of Intelligence and Security; or
(b) any other person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

***impairment of electronic communication to or from a computer*** includes:

(a) the prevention of any such communication; and
(b) the impairment of any such communication on an electronic link or network used by the computer;

but does not include a mere interception of any such communication.

***inland waters*** means waters within Australia other than waters of the sea.

***insurance business*** has the same meaning as in the *Insurance Act 1973*.

***internet carriage service*** means a listed carriage service that enables end-users to access the internet.

***life insurance business*** has the same meaning as in the *Life Insurance Act 1995*.

***liquid fuel*** has the same meaning as in the *Liquid Fuel Emergency Act 1984*.

***listed carriage service*** has the same meaning as in the *Telecommunications Act 1997*.

***local hospital network*** has the same meaning as in the *National Health Reform Act 2011*.

***managed service provider***, in relation to an asset, means an entity that:

(a) manages:
  (i) the asset; or
  (ii) a part of the asset; or
(b) manages an aspect of:
  (i) the asset; or
  (ii) a part of the asset; or
(c) manages an aspect of the operation of:
  (i) the asset; or
  (ii) a part of the asset.

***medical supplies*** includes:

(a) goods for therapeutic use; and
(b) things specified in the rules.

***Ministerial authorisation*** means an authorisation under section 35AB.

***modification***:

(a) in respect of computer data—means:

(i) the alteration or removal of the data; or
(ii) an addition to the data; or

(b) in respect of a computer program—means:
(i) the alteration or removal of the program; or
(ii) an addition to the program.

***national broadcasting service*** has the same meaning as in the *Broadcasting Services Act 1992*.

***National Register of Higher Education Providers*** means the register established and maintained under section 198 of the *Tertiary Education Quality and Standards Agency Act 2011*.

***notification provision*** means:
(a) subsection 35AE(3); or
(b) subsection 35AE(4); or
(c) subsection 35AE(5); or
(d) subsection 35AE(6); or
(e) subsection 35AE(7); or
(f) subsection 35AE(8); or
(g) subsection 35AH(5); or
(h) subsection 35AH(6); or
(i) subsection 35AH(7); or
(j) subsection 35AY(3); or
(k) subsection 35AY(4); or
(l) subsection 35AY(5); or
(m) subsection 35AY(6); or
(n) subsection 35AY(7); or
(o) subsection 35AY(8); or
(p) subsection 51(3); or
(q) subsection 52(4).

***Ombudsman official*** means:
(a) the Ombudsman; or
(b) a Deputy Commonwealth Ombudsman; or
(c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

## 8 Section 5 (paragraph (b) of the definition of *operator*)

Repeal the paragraph, substitute:

(b) for a critical infrastructure asset other than a critical port—an entity that operates the asset or part of the asset.

## 9 Section 5

Insert:

***payment system*** has the same meaning as in the *Payment Systems (Regulation) Act 1998*.

## 10 Section 5

Insert:

***Power and Water Corporation*** means the Power and Water Corporation established by section 4 of the *Power and Water Corporation Act 1987* (NT).

## 11 Section 5 (after paragraph (b) of the definition of *protected information*)

Insert:

(bb) records or is the fact that the Minister has:
  (i) given a Ministerial authorisation; or
  (ii) revoked a Ministerial authorisation; or

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

(bi) 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

(bj) records or is the fact that the Secretary has:
  (i) given a direction under section 35AK; or
  (ii) revoked such a direction; or

(bk) records or is the fact that the Secretary has:
  (i) given a direction under section 35AQ; or
  (ii) revoked such a direction; or

(bl) records or is the fact that the Secretary has:
  (i) given a request under section 35AX; or
  (ii) revoked such a request; or

## 12 Section 5 (paragraph (c) of the definition of *protected information*)

Omit "or (b)", substitute ", (b), (ba), (bb), (bc), (bd), (be), (bf), (bg), (bh), (bi), (bj), (bk) or (bl)".

## 13 Section 5

Insert:

***radiocommunications transmitter*** has the same meaning as in the *Radiocommunications Act 1992*.

***regional centre*** means a city, or a town that has a population of 10,000 or more people.

***Regional Power Corporation*** means the Regional Power Corporation established by section 4 of the *Electricity Corporations Act 2005* (WA).

***registrable superannuation entity*** has the same meaning as in the *Superannuation Industry (Supervision) Act 1993*.

***regulated air cargo agent*** has the same meaning as in the *Aviation Transport Security Act 2004*.

***related body corporate*** has the same meaning as in the *Corporations Act 2001*.

***relevant Commonwealth regulator*** means:

(a) a Department that is specified in the rules; or

(b) a body that is:

(i) established by a law of the Commonwealth; and

(ii) specified in the rules.

***relevant entity***, in relation to an asset, means an entity that:

(a) is the responsible entity for the asset; or

(b) is a direct interest holder in relation to the asset; or

(c) is an operator of the asset; or

(d) is a managed service provider for the asset.

***relevant impact*** has the meaning given by section 8G.

## 14 Section 5 (definition of *relevant industry*)

Repeal the definition.

## 15 Section 5 (definition of *responsible entity*)

Repeal the definition, substitute:

***responsible entity***, for an asset, has the meaning given by section 12L.

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

Omit "sections 10 and 12", substitute "the definition of ***critical energy market operator asset*** and sections 10, 12, 12A, 12D, 12G, 12H, 12J, 12M and 12N".

## 17 Section 5 (paragraph (b) of the definition of *security*)

Omit "sections 10 and 12", substitute "the definition of ***critical energy market operator asset*** and sections 10, 12, 12A, 12D, 12G, 12H, 12J, 12M and 12N".

## 18 Section 5

Insert:

***significant financial benchmark*** has the same meaning as in the *Corporations Act 2001*.

***space technology sector*** means the sector of the Australian economy that involves the commercial provision of space-related services.

Note: The following are examples of space-related services:

(a) position, navigation and timing services in relation to space objects;
(b) space situational awareness services;
(c) space weather monitoring and forecasting;
(d) communications, tracking, telemetry and control in relation to space objects;
(e) remote sensing earth observations from space;
(f) facilitating access to space.

***staff member***, in relation to the authorised agency, means a staff member of ASD (within the meaning of the *Intelligence Services Act 2001*).

***technical assistance notice*** has the same meaning as in Part 15 of the *Telecommunications Act 1997*.

***technical assistance request*** has the same meaning as in Part 15 of the *Telecommunications Act 1997*.

***technical capability notice*** has the same meaning as in Part 15 of the *Telecommunications Act 1997*.

***telecommunications network*** has the same meaning as in the *Telecommunications Act 1997*.

***therapeutic use*** has the same meaning as in the *Therapeutic Goods Act 1989*.

***transport sector*** means the sector of the Australian economy that involves:

(a) owning or operating assets that are used in connection with the transport of goods or passengers on a commercial basis; or

(b) the transport of goods or passengers on a commercial basis.

***unauthorised access, modification or impairment*** has the meaning given by section 12N.

***water and sewerage sector*** means the sector of the Australian economy that involves:

(a) operating water or sewerage systems or networks; or

(b) manufacturing or supplying goods, or providing services, for use in connection with the operation of water or sewerage systems or networks.

## 19 Section 5 (definition of *water utility*)

After "water services", insert "or sewerage services, or both".

## 20 At the end of section 6

Add:

*Interest and control information provided by the Commonwealth*

(5) If the first entity:

(a) is the Governor-General, the Prime Minister or a Minister; and

(b) is a direct interest holder in relation to an asset because of paragraph 8(1)(b);

the first entity is not required to provide any interest and control information.

Note: The expression ***Minister*** is defined in section 2B of the *Acts Interpretation Act 1901*.

(6) However, subsection (5) does not affect the obligation of the Commonwealth to provide interest and control information in relation to the asset if the Commonwealth is also a direct interest holder in relation to the asset because of paragraph 8(1)(a) or (b).

## 21 After section 8C

Insert:

### 8D Meaning of *critical infrastructure sector*

Each of the following sectors of the Australian economy is a ***critical infrastructure sector***:

(a) the communications sector;

(b) the data storage or processing sector;

(c) the financial services and markets sector;

(d) the water and sewerage sector;

(e) the energy sector;

(f) the health care and medical sector;

(g) the higher education and research sector;

(h) the food and grocery sector;

(i) the transport sector;

(j) the space technology sector;

(k) the defence industry sector.

### 8E Meaning of *critical infrastructure sector asset*

(1) An asset is a ***critical infrastructure sector asset*** if it is an asset that relates to a critical infrastructure sector.

*Deeming—when asset relates to a sector*

(2) For the purposes of this Act, each of the following assets is taken to relate to the communications sector:
  (a) a critical telecommunications asset;
  (b) a critical broadcasting asset;
  (c) a critical domain name system.

(3) For the purposes of this Act, a critical data storage or processing asset is taken to relate to the data storage or processing sector.

(4) For the purposes of this Act, each of the following assets is taken to relate to the financial services and markets sector:
  (a) a critical banking asset;
  (b) a critical superannuation asset;
  (c) a critical insurance asset;
  (d) a critical financial market infrastructure asset.

(5) For the purposes of this Act, a critical water asset is taken to relate to the water and sewerage sector.

(6) For the purposes of this Act, each of the following assets is taken to relate to the energy sector:
  (a) a critical electricity asset;
  (b) a critical gas asset;
  (c) a critical energy market operator asset;
  (d) a critical liquid fuel asset.

(7) For the purposes of this Act, a critical hospital is taken to relate to the health care and medical sector.

(8) For the purposes of this Act, a critical education asset is taken to relate to the higher education and research sector.

(9) For the purposes of this Act, a critical food and grocery asset is taken to relate to the food and grocery sector.

(10) For the purposes of this Act, each of the following assets is taken to relate to the transport sector:
  (a) a critical port;
  (b) a critical freight infrastructure asset;

(c) a critical freight services asset;
(d) a critical public transport asset;
(e) a critical aviation asset.

(11) For the purposes of this Act, a critical defence industry asset is taken to relate to the defence industry sector.

## 8F Critical infrastructure sector for a critical infrastructure asset

For the purposes of this Act, the critical infrastructure sector for a critical infrastructure asset is the critical infrastructure sector to which the asset relates.

## 8G Meaning of *relevant impact*

(1) Each of the following is a ***relevant impact*** of a hazard on a critical infrastructure asset:
(a) the impact (whether direct or indirect) of the hazard on the availability of the asset;
(b) the impact (whether direct or indirect) of the hazard on the integrity of the asset;
(c) the impact (whether direct or indirect) of the hazard on the reliability of the asset;
(d) the impact (whether direct or indirect) of the hazard on the confidentiality of:
(i) information about the asset; or
(ii) if information is stored in the asset—the information; or
(iii) if the asset is computer data—the computer data.

(2) Each of the following is a ***relevant impact*** of a cyber security incident on a critical infrastructure asset:
(a) the impact (whether direct or indirect) of the incident on the availability of the asset;
(b) the impact (whether direct or indirect) of the incident on the integrity of the asset;
(c) the impact (whether direct or indirect) of the incident on the reliability of the asset;
(d) the impact (whether direct or indirect) of the incident on the confidentiality of:

(i) information about the asset; or
(ii) if information is stored in the asset—the information; or
(iii) if the asset is computer data—the computer data.

## 22 Paragraphs 9(1)(a), (b), (c) and (d)

Repeal the paragraphs, substitute:

(a) a critical telecommunications asset; or
(b) a critical broadcasting asset; or
(c) a critical domain name system; or
(d) a critical data storage or processing asset; or
(da) a critical banking asset; or
(db) a critical superannuation asset; or
(dc) a critical insurance asset; or
(dd) a critical financial market infrastructure asset; or
(de) a critical water asset; or
(df) a critical electricity asset; or
(dg) a critical gas asset; or
(dh) a critical energy market operator asset; or
(di) a critical liquid fuel asset; or
(dj) a critical hospital; or
(dk) a critical education asset; or
(dl) a critical food and grocery asset; or
(dm) a critical port; or
(dn) a critical freight infrastructure asset; or
(do) a critical freight services asset; or
(dp) a critical public transport asset; or
(dq) a critical aviation asset; or
(dr) a critical defence industry asset; or

## 23 At the end of subsection 9(1)

Add:

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

## 24 Paragraphs 9(2)(a), (b), (c) and (d)

Repeal the paragraphs, substitute:

(a) a critical telecommunications asset; or
(b) a critical broadcasting asset; or
(c) a critical domain name system; or
(d) a critical data storage or processing asset; or
(e) a critical banking asset; or
(f) a critical superannuation asset; or
(g) a critical insurance asset; or
(h) a critical financial market infrastructure asset; or
(i) a critical water asset; or
(j) a critical electricity asset; or
(k) a critical gas asset; or
(l) a critical energy market operator asset; or
(m) a critical liquid fuel asset; or
(n) a critical hospital; or
(o) a critical education asset; or
(p) a critical food and grocery asset; or
(q) a critical port; or
(r) a critical freight infrastructure asset; or
(s) a critical freight services asset; or
(t) a critical public transport asset; or
(u) a critical aviation asset; or
(v) a critical defence industry asset;

## 25 At the end of subsection 9(2)

Add:

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

## 26 After subsection 9(2)

Insert:

(2A) If an asset is owned by:
(a) the Commonwealth; or
(b) a body corporate established by a law of the Commonwealth (other than a government business enterprise);
the asset is not a critical infrastructure asset unless:

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

(d) the asset is prescribed by the rules for the purposes of paragraph (1)(f).

(2B) An asset is not a critical infrastructure asset if, or to the extent to which, the asset is located outside Australia.

## 27 Paragraph 9(3)(b)

Repeal the paragraph, substitute:

(b) the asset relates to a critical infrastructure sector.

## 28 Subparagraph 9(4)(a)(i)

Before "located", insert "wholly or partly".

## 29 Subparagraph 9(4)(a)(ii)

Omit "industry for the asset", substitute "critical infrastructure sector".

## 30 Paragraph 10(1)(a)

After "customers", insert "or any other number of customers prescribed by the rules".

## 31 Paragraph 12(1)(b)

Repeal the paragraph, substitute:

(b) a gas storage facility that has a maximum daily withdrawal capacity of at least 75 terajoules per day or any other maximum daily withdrawal capacity prescribed by the rules;

## 32 After section 12

Insert:

### 12A Meaning of *critical liquid fuel asset*

(1) An asset is a ***critical liquid fuel asset*** if it is any of the following:

(a) a liquid fuel refinery that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (2);

(b) a liquid fuel pipeline that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (3);

(c) a liquid fuel storage facility that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (4).

Note: The rules may prescribe that a specified critical liquid fuel asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(a), the rules may prescribe:

(a) specified liquid fuel refineries that are critical to ensuring the security and reliability of a liquid fuel market; or

(b) requirements for a liquid fuel refinery to be critical to ensuring the security and reliability of a liquid fuel market.

(3) For the purposes of paragraph (1)(b), the rules may prescribe:

(a) specified liquid fuel pipelines that are critical to ensuring the security and reliability of a liquid fuel market; or

(b) requirements for a liquid fuel pipeline to be critical to ensuring the security and reliability of a liquid fuel market.

(4) For the purposes of paragraph (1)(c), the rules may prescribe:

(a) specified liquid fuel storage facilities that are critical to ensuring the security and reliability of a liquid fuel market; or

(b) requirements for a liquid fuel storage facility to be critical to ensuring the security and reliability of a liquid fuel market.

## 12B Meaning of *critical freight infrastructure asset*

(1) An asset is a ***critical freight infrastructure asset*** if it is any of the following:

(a) a road network that, in accordance with subsection (2), functions as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres;

(b) a rail network that, in accordance with subsection (3), functions as a critical corridor for the transportation of goods between:
  (i) 2 States; or
  (ii) a State and a Territory; or
  (iii) 2 Territories; or
  (iv) 2 regional centres;
(c) an intermodal transfer facility that, in accordance with subsection (4), is critical to the transportation of goods between:
  (i) 2 States; or
  (ii) a State and a Territory; or
  (iii) 2 Territories; or
  (iv) 2 regional centres.

Note: The rules may prescribe that a specified critical freight infrastructure asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(a), the rules may prescribe:
(a) specified road networks that function as a critical corridor for the transportation of goods between:
  (i) 2 States; or
  (ii) a State and a Territory; or
  (iii) 2 Territories; or
  (iv) 2 regional centres; or
(b) requirements for a road network to function as a critical corridor for the transportation of goods between:
  (i) 2 States; or
  (ii) a State and a Territory; or
  (iii) 2 Territories; or
  (iv) 2 regional centres.

(3) For the purposes of paragraph (1)(b), the rules may prescribe:
(a) specified rail networks that function as a critical corridor for the transportation of goods between:
  (i) 2 States; or
  (ii) a State and a Territory; or
  (iii) 2 Territories; or

(iv) 2 regional centres; or

(b) requirements for a rail network to function as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres.

(4) For the purposes of paragraph (1)(c), the rules may prescribe:

(a) specified intermodal transfer facilities that are critical to the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres; or

(b) requirements for an intermodal transfer facility to be critical to the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres.

(5) For the purposes of this section, ***road network*** includes a part of a road network.

(6) For the purposes of this section, ***rail network*** includes a part of a rail network.

## 12C Meaning of *critical freight services asset*

(1) An asset is a ***critical freight services asset*** if it is a network that is used by an entity carrying on a business that, in accordance with subsection (2), is critical to the transportation of goods by any or all of the following:

(a) road;

(b) rail;

(c) inland waters;

(d) sea.

Note: The rules may prescribe that a specified critical freight services asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of subsection (1), the rules may prescribe:

(a) specified businesses that are critical to the transportation of goods by any or all of the following:

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea; or

(b) requirements for a business to be critical to the transportation of goods by any or all of the following:

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea.

## 12D Meaning of *critical financial market infrastructure asset*

(1) An asset is a ***critical financial market infrastructure asset*** if it is any of the following assets:

(a) an asset that:

(i) is owned or operated by an Australian body corporate that holds an Australian market licence; and

(ii) is used in connection with the operation of a financial market that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector;

(b) an asset that:

(i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian market licence; and

(ii) is used in connection with the operation of a financial market that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector;

(c) an asset that:

(i) is owned or operated by an Australian body corporate that holds an Australian CS facility licence; and

(ii) is used in connection with the operation of a clearing and settlement facility that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector;

(d) an asset that:

(i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian CS facility licence; and

(ii) is used in connection with the operation of a clearing and settlement facility that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector;

(e) an asset that:

(i) is owned or operated by an Australian body corporate that holds a benchmark administrator licence; and

(ii) is used in connection with the administration of a significant financial benchmark that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector;

(f) an asset that:

(i) is owned or operated by an associated entity of an Australian body corporate that holds a benchmark administrator licence; and

(ii) is used in connection with the administration of a significant financial benchmark that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector;

(g) an asset that:

(i) is owned or operated by an Australian body corporate that holds an Australian derivative trade repository licence; and

(ii) is used in connection with the operation of a derivative trade repository that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector;

(h) an asset that:

(i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian derivative trade repository licence; and

(ii) is used in connection with the operation of a derivative trade repository that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector;

(i) an asset that is used in connection with the operation of a payment system that, in accordance with subsection (6), is critical to the security and reliability of the financial services and markets sector.

Note: The rules may prescribe that a specified critical financial market infrastructure asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraphs (1)(a) and (b), the rules may prescribe:

(a) specified financial markets that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a financial market to be critical to the security and reliability of the financial services and markets sector.

(3) For the purposes of paragraphs (1)(c) and (d), the rules may prescribe:

(a) specified clearing and settlement facilities that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a clearing and settlement facility to be critical to the security and reliability of the financial services and markets sector.

(4) For the purposes of paragraphs (1)(e) and (f), the rules may prescribe:

(a) specified significant financial benchmarks that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a significant financial benchmark to be critical to the security and reliability of the financial services and markets sector.

(5) For the purposes of paragraphs (1)(g) and (h), the rules may prescribe:

(a) specified derivative trade repositories that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a derivative trade repository to be critical to the security and reliability of the financial services and markets sector.

(6) For the purposes of paragraph (1)(i), the rules may prescribe:

(a) specified payment systems that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a payment system to be critical to the security and reliability of the financial services and markets sector.

(7) For the purposes of this section, ***Australian body corporate*** means a body corporate that is incorporated in Australia.

## 12E Meaning of *critical broadcasting asset*

(1) One or more broadcasting transmission assets are a ***critical broadcasting asset*** if:

(a) the broadcasting transmission assets are:

(i) owned or operated by the same entity; and

(ii) located on a site that, in accordance with subsection (2), is a critical transmission site; or

(b) the broadcasting transmission assets are:

(i) owned or operated by the same entity; and

(ii) located on at least 50 different sites; and

(iii) not broadcasting re-transmission assets; or

(c) the broadcasting transmission assets are owned or operated by an entity that, in accordance with subsection (3), is critical to the transmission of a broadcasting service.

Note: The rules may prescribe that a specified critical broadcasting asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(a), the rules may prescribe:

(a) specified sites that are critical transmission sites; or

(b) requirements for sites to be critical transmission sites.

(3) For the purposes of paragraph (1)(c), the rules may prescribe:

(a) specified entities that are critical to the transmission of a broadcasting service; or

(b) requirements for an entity to be critical to the transmission of a broadcasting service.

## 12F Meaning of *critical data storage or processing asset*

(1) An asset is a ***critical data storage or processing asset*** if:

(a) it is owned or operated by an entity that is a data storage or processing provider; and

(b) it is used wholly or primarily to provide a data storage or processing service that is provided by the entity on a commercial basis to an end-user that is:

(i) the Commonwealth; or

(ii) a body corporate established by a law of the Commonwealth; or

(iii) a State; or

(iv) a body corporate established by a law of a State; or

(v) a Territory; or

(vi) a body corporate established by a law of a Territory; and

(c) the entity knows that the asset is used as described in paragraph (b).

Note: The rules may prescribe that a specified critical data storage or processing asset is not a critical infrastructure asset (see section 9).

(2) An asset is a ***critical data storage or processing asset*** if:

(a) it is owned or operated by an entity that is a data storage or processing provider; and

(b) it is used wholly or primarily to provide a data storage or processing service that:

(i) is provided by the entity on a commercial basis to an end-user that is the responsible entity for a critical infrastructure asset; and

(ii) relates to business critical data; and

(c) the entity knows that the asset is used as described in paragraph (b).

Note: The rules may prescribe that a specified critical data storage or processing asset is not a critical infrastructure asset (see section 9).

(3) If:

(a) an entity (the ***first entity***) is the responsible entity for a critical infrastructure asset; and

(b) the first entity becomes aware that a data storage or processing service:

(i) is provided by another entity on a commercial basis to the first entity; and

(ii) relates to business critical data;

the first entity must:

(c) take reasonable steps to inform that other entity that the first entity has become aware that the data storage or processing service:

(i) is provided by the other entity on a commercial basis to the first entity; and

(ii) relates to business critical data; and

(d) do so as soon as practicable after becoming so aware.

Civil penalty for contravention of this subsection: 50 penalty units.

## 12G Meaning of *critical banking asset*

(1) An asset is a ***critical banking asset*** if it is any of the following assets:

(a) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by an authorised deposit-taking institution;

(ii) the authorised deposit-taking institution is an authorised deposit-taking institution that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of banking business;

(b) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by a body corporate that is a related body corporate of an authorised deposit-taking institution;

(ii) the body corporate is a body corporate that, in accordance with subsection (3), is critical to the security

and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of banking business.

Note: The rules may prescribe that a specified critical banking asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of subparagraph (1)(a)(ii), the rules may prescribe:

(a) specified authorised deposit-taking institutions that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for an authorised deposit-taking institution to be critical to the security and reliability of the financial services and markets sector.

(3) For the purposes of subparagraph (1)(b)(ii), the rules may prescribe:

(a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

## 12H Meaning of *critical insurance asset*

(1) An asset is a ***critical insurance asset*** if it is any of the following assets:

(a) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by an entity that carries on insurance business;

(ii) the entity is an entity that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of insurance business;

(b) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by a body corporate that is a related body corporate of an entity that carries on insurance business;

(ii) the body corporate is a body corporate that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of insurance business;

(c) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by an entity that carries on life insurance business;

(ii) the entity is an entity that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of life insurance business;

(d) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by a body corporate that is a related body corporate of an entity that carries on life insurance business;

(ii) the body corporate is a body corporate that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of life insurance business;

(e) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by an entity that carries on health insurance business;

(ii) the entity is an entity that, in accordance with subsection (6), is critical to the security and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of health insurance business;

(f) an asset where the following conditions are satisfied:

(i) the asset is owned or operated by a body corporate that is a related body corporate of an entity that carries on health insurance business;

(ii) the body corporate is a body corporate that, in accordance with subsection (7), is critical to the security

and reliability of the financial services and markets sector;

(iii) the asset is used in connection with the carrying on of health insurance business.

Note: The rules may prescribe that a specified critical insurance asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of subparagraph (1)(a)(ii), the rules may prescribe:

(a) specified entities that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector.

(3) For the purposes of subparagraph (1)(b)(ii), the rules may prescribe:

(a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

(4) For the purposes of subparagraph (1)(c)(ii), the rules may prescribe:

(a) specified entities that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector.

(5) For the purposes of subparagraph (1)(d)(ii), the rules may prescribe:

(a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

(6) For the purposes of subparagraph (1)(e)(ii), the rules may prescribe:

(a) specified entities that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector.

(7) For the purposes of subparagraph (1)(f)(ii), the rules may prescribe:

(a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

## 12J Meaning of *critical superannuation asset*

(1) An asset is a ***critical superannuation asset*** if:

(a) it is owned or operated by a registrable superannuation entity that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; and

(b) it is used in connection with the operation of a superannuation fund.

Note: The rules may prescribe that a specified critical superannuation asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(a), the rules may prescribe:

(a) specified registrable superannuation entities that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a registrable superannuation entity to be critical to the security and reliability of the financial services and markets sector.

## 12K Meaning of *critical food and grocery asset*

(1) An asset is a ***critical food and grocery asset*** if it is a network that:

(a) is used for the distribution or supply of:

(i) food; or

(ii) groceries; and

(b) is owned or operated by an entity that is:

(i) a critical supermarket retailer, in accordance with subsection (2); or

(ii) a critical food wholesaler, in accordance with subsection (3); or

(iii) a critical grocery wholesaler, in accordance with subsection (4).

Note: The rules may prescribe that a specified critical food and grocery asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of subparagraph (1)(b)(i), the rules may prescribe:

(a) specified entities that are critical supermarket retailers; or

(b) requirements for an entity to be a critical supermarket retailer.

(3) For the purposes of subparagraph (1)(b)(ii), the rules may prescribe:

(a) specified entities that are critical food wholesalers; or

(b) requirements for an entity to be a critical food wholesaler.

(4) For the purposes of subparagraph (1)(b)(iii), the rules may prescribe:

(a) specified entities that are critical grocery wholesalers; or

(b) requirements for an entity to be a critical grocery wholesaler.

## 12KA Meaning of *critical domain name system*

(1) An asset is a ***critical domain name system*** if it:

(a) is managed by an entity that, in accordance with subsection (2), is critical to the administration of an Australian domain name system; and

(b) is used in connection with the administration of an Australian domain name system.

Note: The rules may prescribe that a specified critical domain name system is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(a), the rules may prescribe:

(a) specified entities that are critical to the administration of an Australian domain name system; or

(b) requirements for an entity to be critical to the administration of an Australian domain name system.

## 12L Meaning of *responsible entity*

*Critical telecommunications asset*

(1) The responsible entity for a critical telecommunications asset is:
  (a) whichever of the following is applicable:
    (i) if the critical telecommunications asset is owned or operated by a carrier—the carrier;
    (ii) if the critical telecommunications asset is owned or operated by a carriage service provider—the carriage service provider; or
  (b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical broadcasting asset*

(2) The responsible entity for a critical broadcasting asset is:
  (a) the entity referred to in whichever of the following provisions is applicable:
    (i) subparagraph 12E(1)(a)(i);
    (ii) subparagraph 12E(1)(b)(i);
    (iii) paragraph 12E(1)(c); or
  (b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical domain name system*

(3) The responsible entity for a critical domain name system is:
  (a) the entity referred to in paragraph 12KA(1)(a); or
  (b) if another entity is prescribed by the rules in relation to the system—that other entity.

*Critical data storage or processing asset*

(4) The responsible entity for a critical data storage or processing asset is:
  (a) if the asset is covered by subsection 12F(1)—the entity referred to in paragraph 12F(1)(a); or
  (b) if the asset is covered by subsection 12F(2)—the entity referred to in paragraph 12F(2)(a); or

(c) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical banking asset*

(5) The responsible entity for a critical banking asset is:
(a) if the asset is covered by paragraph 12G(1)(a)—the authorised deposit-taking institution referred to in subparagraph 12G(1)(a)(i); or
(b) if the asset is covered by paragraph 12G(1)(b)—the body corporate referred to in subparagraph 12G(1)(b)(i); or
(c) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical superannuation asset*

(6) The responsible entity for a critical superannuation asset is:
(a) the registrable superannuation entity referred to in subsection 12J(1); or
(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical insurance asset*

(7) The responsible entity for a critical insurance asset is:
(a) if the asset is covered by paragraph 12H(1)(a)—the entity referred to in subparagraph 12H(1)(a)(i); or
(b) if the asset is covered by paragraph 12H(1)(b)—the body corporate referred to in subparagraph 12H(1)(b)(i); or
(c) if the asset is covered by paragraph 12H(1)(c)—the entity referred to in subparagraph 12H(1)(c)(i); or
(d) if the asset is covered by paragraph 12H(1)(d)—the body corporate referred to in subparagraph 12H(1)(d)(i); or
(e) if the asset is covered by paragraph 12H(1)(e)—the entity referred to in subparagraph 12H(1)(e)(i); or
(f) if the asset is covered by paragraph 12H(1)(f)—the body corporate referred to in subparagraph 12H(1)(f)(i); or
(g) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical financial market infrastructure asset*

(8) The responsible entity for a critical financial market infrastructure asset is:

(a) if the asset is covered by paragraph 12D(1)(a)—the body corporate referred to in subparagraph 12D(1)(a)(i); or

(b) if the asset is covered by paragraph 12D(1)(b)—the associated entity referred to in subparagraph 12D(1)(b)(i); or

(c) if the asset is covered by paragraph 12D(1)(c)—the body corporate referred to in subparagraph 12D(1)(c)(i); or

(d) if the asset is covered by paragraph 12D(1)(d)—the associated entity referred to in subparagraph 12D(1)(d)(i); or

(e) if the asset is covered by paragraph 12D(1)(e)—the body corporate referred to in subparagraph 12D(1)(e)(i); or

(f) if the asset is covered by paragraph 12D(1)(f)—the associated entity referred to in subparagraph 12D(1)(f)(i); or

(g) if the asset is covered by paragraph 12D(1)(g)—the body corporate referred to in subparagraph 12D(1)(g)(i); or

(h) if the asset is covered by paragraph 12D(1)(h)—the associated entity referred to in subparagraph 12D(1)(h)(i); or

(i) if the asset is covered by paragraph 12D(1)(i)—the entity prescribed by the rules; or

(j) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical water asset*

(9) The responsible entity for a critical water asset is:

(a) the water utility that holds the licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory, to provide the service to be delivered by the asset; or

(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical electricity asset*

(10) The responsible entity for a critical electricity asset is:

(a) the entity that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset; or
(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical gas asset*

(11) The responsible entity for a critical gas asset is:
(a) the entity that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset; or
(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical energy market operator asset*

(12) The responsible entity for a critical energy market operator asset is:
(a) if the asset is used by Australian Energy Market Operator Limited (ACN 072 010 327)—that company; or
(b) if the asset is used by Power and Water Corporation—that corporation; or
(c) if the asset is used by Regional Power Corporation—that corporation; or
(d) if the asset is used by Electricity Networks Corporation—that corporation; or
(e) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical liquid fuel asset*

(13) The responsible entity for a critical liquid fuel asset is:
(a) if the asset is a liquid fuel refinery—the entity that operates the liquid fuel refinery; or
(b) if the asset is a liquid fuel pipeline—the entity that operates the liquid fuel pipeline; or
(c) if the asset is a liquid fuel storage facility—the entity that operates the liquid fuel storage facility; or
(d) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical hospital*

(14) The responsible entity for a critical hospital is:
(a) if the critical hospital is a public hospital—the local hospital network that operates the hospital; or
(b) if the critical hospital is a private hospital—the entity that holds the licence, approval or authorisation (however described), under a law of a State or a Territory to operate the hospital; or
(c) if another entity is prescribed by the rules in relation to the hospital—that other entity.

*Critical education asset*

(15) The responsible entity for a critical education asset is:
(a) the entity referred to in the definition of ***critical education asset*** in section 5; or
(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical food and grocery asset*

(16) The responsible entity for a critical food and grocery asset is:
(a) the entity referred to in paragraph 12K(1)(b); or
(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical port*

(17) The responsible entity for a critical port is:
(a) the port operator (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003*) of the port; or
(b) if another entity is prescribed by the rules in relation to the port—that other entity.

*Critical freight infrastructure asset*

(18) The responsible entity for a critical freight infrastructure asset is:
(a) if the Commonwealth is responsible for the management of the asset—the Commonwealth; or

(b) if a State is responsible for the management of the asset—the State; or

(c) if a Territory is responsible for the management of the asset—the Territory; or

(d) if a body is:

(i) established by a law of the Commonwealth, a State or a Territory; and

(ii) responsible for the management of the asset;

that body; or

(e) if none of paragraphs (a), (b), (c), (d) and (e) apply—the entity prescribed by the rules in relation to the asset; or

(f) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical freight services asset*

(19) The responsible entity for a critical freight services asset is:

(a) the entity referred to in subsection 12C(1); or

(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical public transport asset*

(20) The responsible entity for a critical public transport asset is:

(a) the entity referred to in paragraph (a) of the definition of ***critical public transport asset*** in section 5; or

(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical aviation asset*

(21) The responsible entity for a critical aviation asset is:

(a) if the asset is:

(i) used in connection with the provision of an air service; and

(ii) owned or operated by an aircraft operator;

the aircraft operator; or

(b) if the asset is:

(i) used in connection with the provision of an air service; and

(ii) owned or operated by a regulated air cargo agent;

the regulated air cargo agent; or

(c) if the asset is used by an airport operator in connection with the operation of an airport—the airport operator; or

(d) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Critical defence industry asset*

(22) The responsible entity for a critical defence industry asset is:

(a) the entity referred to in paragraph (a) of the definition of ***critical defence industry asset***; or

(b) if another entity is prescribed by the rules in relation to the asset—that other entity.

*Assets prescribed by the rules*

(23) The responsible entity for an asset prescribed by the rules in relation to the asset for the purposes of paragraph 9(1)(f) is the entity specified in the rules.

*Assets declared to be a critical infrastructure asset*

(24) The responsible entity for an asset declared under section 51 to be a critical infrastructure asset is the entity specified in the declaration as the responsible entity for the asset (see subsection 51(2)).

## 12M Meaning of *cyber security incident*

A ***cyber security incident*** is one or more acts, events or circumstances involving any of the following:

(a) unauthorised access to:

(i) computer data; or

(ii) a computer program;

(b) unauthorised modification of:

(i) computer data; or

(ii) a computer program;

(c) unauthorised impairment of electronic communication to or from a computer;

(d) unauthorised impairment of the availability, reliability, security or operation of:

(i) a computer; or

(ii) computer data; or

(iii) a computer program.

## 12N Meaning of *unauthorised access, modification or impairment*

(1) For the purposes of this Act:

(a) access to:

(i) computer data; or

(ii) a computer program; or

(b) modification of:

(i) computer data; or

(ii) a computer program; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the availability, reliability, security or operation of:

(i) a computer; or

(ii) computer data; or

(iii) a computer program;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(1A) The following is an example of a situation where a person is not entitled to cause access, modification or impairment of a kind mentioned in subsection (1): a person who is an employee or agent of the responsible entity for an asset would exceed the person's authority as such an employee or agent in causing such access, modification or impairment in relation to the asset.

(2) For the purposes of subsection (1), it is immaterial whether the person can be identified.

(3) For the purposes of subsection (1), if:

(a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

(b) the person does so:

(i) under a warrant issued under a law of the Commonwealth, a State or a Territory; or

(ii) under an emergency authorisation given to the person under Part 3 of the *Surveillance Devices Act 2004* or under a law of a State or Territory that makes provision to similar effect; or

(iii) under a tracking device authorisation given to the person under section 39 of the *Surveillance Devices Act 2004*; or

(iv) in accordance with a technical assistance request; or

(v) in compliance with a technical assistance notice; or

(vi) in compliance with a technical capability notice;

the person is entitled to cause that access, modification or impairment.

### 12P Examples of responding to a cyber security incident

The following are examples of responding to a cyber security incident:

(a) if the incident is imminent—preventing the incident;

(b) mitigating a relevant impact of the incident on:

(i) a critical infrastructure asset; or

(ii) a critical infrastructure sector asset;

(c) if a critical infrastructure asset or a critical infrastructure sector asset has been, or is being, affected by the incident—restoring the functionality of the asset.

## 33 Paragraph 13(1)(b)

Omit "that is a reporting entity for,", insert ", so far as the entity is the responsible entity for, a reporting entity for, a relevant entity for,".

## 34 At the end of paragraph 13(1)(b)

Add:

or (iv) used in the course of, or in relation to, banking to which paragraph 51(xiii) of the Constitution applies; or

(v) used in the course of, or in relation to, insurance to which paragraph 51(xiv) of the Constitution applies; or

(vi) used to supply a carriage service; or

(vii) used in connection with the provision of a broadcasting service; or

(viii) used to administer a domain name system;

## 35 Subsection 13(2)

Omit "also applies", substitute "and section 60AA (acquisition of property) also apply".

## 36 Division 1 of Part 2 (heading)

Omit "**Simplified outline of this Part**", substitute "**Introduction**".

## 37 At the end of section 18

Add:

Note: See also section 18A (application of this Part).

## 38 At the end of Division 1 of Part 2

Add:

### 18A Application of this Part

(1) This Part applies to a critical infrastructure asset if:

(a) the asset is specified in the rules; or

(b) both:

(i) the asset is the subject of a declaration under section 51; and

(ii) the declaration determines that this Part applies to the asset; or

(c) immediately before the commencement of this section, the asset was a critical infrastructure asset (within the meaning of this Act as in force immediately before that commencement).

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

(2) Subsection (1) has effect subject to subsection (3).

(3) The rules may provide that, if an asset becomes a critical infrastructure asset, this Part does not apply to the asset during the period:
  (a) beginning when the asset became a critical infrastructure asset; and
  (b) ending at a time ascertained in accordance with the rules.

### 18AA Consultation—rules

*Scope*

(1) This section applies to rules made for the purposes of section 18A.

*Consultation*

(2) Before making or amending the rules, the Minister must:
  (a) cause to be published on the Department's website a notice:
    (i) setting out the draft rules or amendments; and
    (ii) inviting persons to make submissions to the Minister about the draft rules or amendments within 28 days after the notice is published; and
  (b) give a copy of the notice to each First Minister; and
  (c) consider any submissions received within the 28-day period mentioned in paragraph (a).

### 39 After Part 2

Insert:

# Part 2B—Notification of cyber security incidents

### 30BA Simplified outline of this Part

If a cyber security incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident.

Note: See also section 30BB (application of this Part).

## 30BB Application of this Part

(1) This Part applies to a critical infrastructure asset if:
  (a) the asset is specified in the rules; or
  (b) both:
    (i) the asset is the subject of a declaration under section 51; and
    (ii) the declaration determines that this Part applies to the asset.

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

(2) Subsection (1) has effect subject to subsection (3).

(3) The rules may provide that, if an asset becomes a critical infrastructure asset, this Part does not apply to the asset during the period:
  (a) beginning when the asset became a critical infrastructure asset; and
  (b) ending at a time ascertained in accordance with the rules.

## 30BBA Consultation—rules

*Scope*

(1) This section applies to rules made for the purposes of section 30BB.

*Consultation*

(2) Before making or amending the rules, the Minister must:
  (a) cause to be published on the Department's website a notice:
    (i) setting out the draft rules or amendments; and
    (ii) inviting persons to make submissions to the Minister about the draft rules or amendments within 28 days after the notice is published; and
  (b) give a copy of the notice to each First Minister; and
  (c) consider any submissions received within the 28-day period mentioned in paragraph (a); and

(d) if the Minister is aware that an entity is the responsible entity for an asset that is, or is proposed to be, specified in the rules:
(i) give the entity a copy of the draft rules or amendments; and
(ii) if a submission is received from the entity within the 28-day period mentioned in paragraph (a)—give the entity a written statement that sets out the Minister's response to the submission.

## 30BC Notification of critical cyber security incidents

(1) If:
(a) an entity is the responsible entity for a critical infrastructure asset; and
(b) the entity becomes aware that:
(i) a cyber security incident has occurred or is occurring; and
(ii) the incident has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset;

the entity must:
(c) give the relevant Commonwealth body (see section 30BF) a report that:
(i) is about the incident; and
(ii) includes such information (if any) as is prescribed by the rules; and
(d) do so as soon as practicable, and in any event within 12 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units.

*Form of report etc.*

(2) A report under subsection (1) may be given:
(a) orally; or
(b) in writing.

(3) If a report under subsection (1) is given orally, the entity must:
(a) do both of the following:

(i) make a written record of the report in the approved form;

(ii) give a copy of the written record of the report to the relevant Commonwealth body (see section 30BF); and

(b) do so within 84 hours after the report is given.

Civil penalty: 50 penalty units.

(4) If the report is given in writing, the entity must ensure that the report is in the approved form.

Civil penalty: 50 penalty units.

*Exemption—written record*

(5) The head (however described) of the relevant Commonwealth body (see section 30BF) may, by written notice given to an entity, exempt the entity from subsection (3) in relation to a report about a specified cyber security incident.

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

(6) A notice under subsection (5) is not a legislative instrument.

(7) The head (however described) of the relevant Commonwealth body (see section 30BF) may, by writing, delegate any or all of the head's powers under subsection (5) to a person who:

(a) is an SES employee, or acting SES employee, in the relevant Commonwealth body; or

(b) holds, or is acting in, a position in the relevant Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

(8) In exercising powers under a delegation, the delegate must comply with any directions of the head (however described) of the relevant Commonwealth body.

## 30BD Notification of other cyber security incidents

(1) If:

(a) an entity is the responsible entity for a critical infrastructure asset; and

(b) the entity becomes aware that:

(i) a cyber security incident has occurred, is occurring or is imminent; and

(ii) the incident has had, is having, or is likely to have, a relevant impact on the asset;

the entity must:

(c) give the relevant Commonwealth body (see section 30BF) a report that:

(i) is about the incident; and

(ii) includes such information (if any) as is prescribed by the rules; and

(d) do so as soon as practicable, and in any event within 72 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units.

*Form of report etc.*

(2) A report under subsection (1) may be given:

(a) orally; or

(b) in writing.

(3) If a report under subsection (1) is given orally, the entity must:

(a) do both of the following:

(i) make a written record of the report in the approved form;

(ii) give a copy of the written record of the report to the relevant Commonwealth body (see section 30BF); and

(b) do so within 48 hours after the report is given.

Civil penalty: 50 penalty units.

(4) If the report is given in writing, the entity must ensure that the report is in the approved form.

Civil penalty: 50 penalty units.

*Exemption—written record*

(5) The head (however described) of the relevant Commonwealth body (see section 30BF) may, by written notice given to an entity, exempt the entity from subsection (3) in relation to a report about a specified cyber security incident.

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

(6) A notice under subsection (5) is not a legislative instrument.

(7) The head (however described) of the relevant Commonwealth body (see section 30BF) may, by writing, delegate any or all of the head's powers under subsection (5) to a person who:

(a) is an SES employee, or acting SES employee, in the relevant Commonwealth body; or

(b) holds, or is acting in, a position in the relevant Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

(8) In exercising powers under a delegation, the delegate must comply with any directions of the head (however described) of the relevant Commonwealth body.

## 30BE Liability

(1) 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 section 30BC or section 30BD.

(2) 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 (1).

## 30BEA Significant impact

For the purposes of this Part, a cyber security incident has a significant impact (whether direct or indirect) on the availability of an asset if, and only if:

(a) both:
(i) the asset is used in connection with the provision of essential goods or services; and
(ii) the incident has materially disrupted the availability of those essential goods or services; or
(b) any of the circumstances specified in the rules exist in relation to the incident.

## 30BEB Consultation—rules

*Scope*

(1) This section applies to rules made for the purposes of paragraph 30BEA(b).

*Consultation*

(2) If the Minister is aware that an entity is the responsible entity for a critical infrastructure asset, then, before making or amending the rules, the Minister must:
(a) give the entity a copy of the draft rules or amendments; and
(b) give the entity a written notice inviting the entity to make a submission to the Minister about the draft rules or amendments within 28 days after the notice is given; and
(c) consider any submission received within the 28-day period mentioned in paragraph (b); and
(d) if a submission is received from the entity within the 28-day period mentioned in paragraph (b)—give the entity a written statement that sets out the Minister's response to the submission.

## 30BF Relevant Commonwealth body

For the purposes of this Part, ***relevant Commonwealth body*** means:
(a) a Department that is specified in the rules; or
(b) a body that is:
(i) established by a law of the Commonwealth; and
(ii) specified in the rules; or

(c) if:

(i) no rules are in force for the purposes of paragraph (a); and

(ii) no rules are in force for the purposes of paragraph (b);

ASD.

## 40 Paragraph 32(4)(c)

Omit "industry for the critical infrastructure asset", substitute "critical infrastructure sector".

## 41 At the end of section 32

Add:

*Other powers not limited*

(6) This section does not, by implication, limit a power conferred by another provision of this Act.

## 42 Subparagraph 33(1)(a)(i)

Before "located", insert "wholly or partly".

## 43 Subparagraph 33(1)(a)(ii)

Omit "industry for the critical infrastructure asset", substitute "critical infrastructure sector".

## 44 At the end of Part 3

Add:

### 35AAB Liability

(1) 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 32(2).

(2) 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 (1) of this section.

### 45 After Part 3

Insert:

# Part 3A—Responding to serious cyber security incidents

## Division 1—Simplified outline of this Part

### 35AA Simplified outline of this Part

- This Part sets up a regime for the Commonwealth to respond to serious cyber security incidents.
- If a cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset, 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 a relevant entity for the asset;
  - (b) authorise the Secretary to give an action direction to a relevant entity for the asset;
  - (c) authorise the Secretary to give an intervention request to the authorised agency.
- An information-gathering direction requires the relevant entity to give information to the Secretary.
- An action direction requires the relevant entity 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 asset.

## Division 2—Ministerial authorisation relating to cyber security incident

### 35AB Ministerial authorisation

*Scope*

(1) This section applies if the Minister is satisfied that:
  (a) a cyber security incident:
    (i) has occurred; or
    (ii) is occurring; or
    (iii) is imminent; and
  (b) the incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset (the ***primary asset***); and
  (c) there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:
    (i) the social or economic stability of Australia or its people; or
    (ii) the defence of Australia; or
    (iii) national security; and
  (d) no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

*Authorisation*

(2) The Minister may, on application by the Secretary, do any or all of the following things:
  (a) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and the primary asset;
  (b) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and a specified critical infrastructure sector asset;
  (c) authorise the Secretary to give to a specified entity a specified direction under section 35AQ that relates to the incident and the primary asset;

(d) authorise the Secretary to give to a specified entity a specified direction under section 35AQ that relates to the incident and a specified critical infrastructure sector asset;

(e) authorise the Secretary to give a specified request under section 35AX that relates to the incident and the primary asset;

(f) authorise the Secretary to give a specified request under section 35AX that relates to the incident and a specified critical infrastructure sector asset.

Note 1: Section 35AK deals with information gathering directions.

Note 2: Section 35AQ deals with action directions.

Note 3: Section 35AX deals with intervention requests.

(3) An authorisation under subsection (2) is to be known as a ***Ministerial authorisation***.

(4) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not apply to subsection (2) of this section.

Note: Subsection 33(3AB) of the *Acts Interpretation Act 1901* deals with specification by class.

*Information gathering directions*

(5) A Ministerial authorisation under paragraph (2)(a) or (b):

(a) is generally applicable to the incident and the asset concerned; and

(b) is to be made without reference to any specific directions.

(6) The Minister must not give a Ministerial authorisation under paragraph (2)(a) or (b) unless the Minister is satisfied that the directions that could be authorised by the Ministerial authorisation are likely to facilitate a practical and effective response to the incident.

*Action directions*

(7) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) unless the Minister is satisfied that:

(a) the specified entity is unwilling or unable to take all reasonable steps to respond to the incident; and

(b) the specified direction is reasonably necessary for the purposes of responding to the incident; and

(c) the specified direction is a proportionate response to the incident; and

(d) compliance with the specified direction is technically feasible.

Note: Section 12P provides examples of responding to a cyber security incident.

(8) In determining whether the specified direction is a proportionate response to the incident, the Minister must have regard to:

(a) the impact of the specified direction on:

(i) the activities carried on by the specified entity; and

(ii) the functioning of the asset concerned; and

(b) the consequences of compliance with the specified direction; and

(c) such other matters (if any) as the Minister considers relevant.

(9) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) if the specified direction:

(a) requires the specified entity to permit the authorised agency to do an act or thing that could be the subject of a request under section 35AX; or

(b) requires the specified entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident.

*Intervention requests*

(10) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) unless the Minister is satisfied that:

(a) giving a Ministerial authorisation under paragraph (2)(c) or (d) would not amount to a practical and effective response to the incident; and

(b) if there is only one relevant entity for the asset concerned—the relevant entity is unwilling or unable to take all reasonable steps to respond to the incident; and

(c) if there are 2 or more relevant entities for the asset concerned—those entities, when considered together, are

unwilling or unable to take all reasonable steps to respond to the incident; and

(d) the specified request is reasonably necessary for the purposes of responding to the incident; and

(e) the specified request is a proportionate response to the incident; and

(f) compliance with the specified request is technically feasible; and

(g) each of the acts or things specified in the specified request is an act or thing of a kind covered by section 35AC.

Note: Section 12P provides examples of responding to a cyber security incident.

(11) In determining whether the specified request is a proportionate response to the incident, the Minister must have regard to:

(a) the impact of compliance with the specified request on the functioning of the asset concerned; and

(b) the consequences of acts or things that would be done in compliance with the specified request; and

(c) such other matters (if any) as the Minister considers relevant.

(12) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) if compliance with the specified request would involve the authorised agency taking offensive cyber action against a person who is directly or indirectly responsible for the incident.

(13) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) unless the Minister has obtained the agreement of:

(a) the Prime Minister; and

(b) the Defence Minister.

(14) An agreement under subsection (13) may be given:

(a) orally; or

(b) in writing.

(15) If an agreement under subsection (13) is given orally, the Prime Minister or the Defence Minister, as the case requires, must:

(a) do both of the following:

(i) make a written record of the agreement;
(ii) give a copy of the written record of the agreement to the Minister; and

(b) do so within 48 hours after the agreement is given.

*Ministerial authorisation is not a legislative instrument*

(16) A Ministerial authorisation is not a legislative instrument.

*Other powers not limited*

(17) This section does not, by implication, limit a power conferred by another provision of this Act.

## 35AC Kinds of acts or things that may be specified in an intervention request

For the purposes of the application of paragraph 35AB(10)(g) to a Ministerial authorisation of a request, each of the following kinds of acts or things is covered by this section:

(a) access or modify:
(i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
(ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(b) undertake an analysis of:
(i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
(ii) a computer program that is, or is part of, the asset to which the Ministerial authorisation relates; or
(iii) computer data that is, or is part of, the asset to which the Ministerial authorisation relates; or
(iv) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(c) if it is necessary to achieve the purpose mentioned in paragraph (b)—install a computer program on a computer that is, or is part of, the asset to which the Ministerial authorisation relates;

(d) access, add, restore, copy, alter or delete data held in:

(i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or

(ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(e) access, restore, copy, alter or delete a computer program that is, or is part of, the asset to which the Ministerial authorisation relates;

(f) access, copy, alter or delete a computer program that is installed on a computer that is, or is part of, the asset to which the Ministerial authorisation relates;

(g) alter the functioning of:

(i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or

(ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(h) remove or disconnect:

(i) a computer; or

(ii) a computer device;

from a computer network that is, or is part of, the asset to which the Ministerial authorisation relates;

(i) connect or add:

(i) a computer; or

(ii) a computer device;

to a computer network that is, or is part of, the asset to which the Ministerial authorisation relates;

(j) remove:

(i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or

(ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

from premises.

## 35AD Consultation

(1) Before giving a Ministerial authorisation under paragraph 35AB(2)(c) or (d), the Minister must consult the specified entity unless the delay that would occur if the specified

entity were consulted would frustrate the effectiveness of the Ministerial authorisation.

(2) Before giving a Ministerial authorisation under paragraph 35AB(2)(e) or (f) in relation to an asset, the Minister must:

(a) if the asset is a critical infrastructure asset—consult the responsible entity for the asset; or

(b) if the asset is a critical infrastructure sector asset (other than a critical infrastructure asset)—consult whichever of the following entities the Minister considers to be most relevant in relation to the proposed authorisation:

(i) the owner, or each of the owners, of the asset;

(ii) the operator, or each of the operators, of the asset;

unless the delay that would occur if the entity or entities were consulted would frustrate the effectiveness of the Ministerial authorisation.

(3) If subsection (1) or (2) requires an entity to be consulted, that consultation must involve:

(a) giving the entity a copy of the draft Ministerial authorisation; and

(b) inviting the entity to make a submission to the Minister about the draft Ministerial authorisation within 24 hours after receiving the copy of the draft Ministerial authorisation.

### 35AE Form and notification of Ministerial authorisation

(1) A Ministerial authorisation may be given:

(a) orally; or

(b) in writing.

(2) The Minister must not give a Ministerial authorisation orally in relation to:

(a) a cyber security incident; and

(b) an asset;

unless the delay that would occur if the Ministerial authorisation were to be made in writing would frustrate the effectiveness of:

(c) any directions that may be given under section 35AK or 35AQ in relation to the incident and the asset; or

(d) any requests that may be given under section 35AX in relation to the incident and the asset.

*Notification of Ministerial authorisations given orally*

(3) If a Ministerial authorisation is given orally in relation to:
(a) a cyber security incident; and
(b) an asset;
the Minister must:
(c) do both of the following:
(i) make a written record of the Ministerial authorisation;
(ii) give a copy of the written record of the Ministerial authorisation to the Secretary and the Inspector-General of Intelligence and Security; and
(d) do so within 48 hours after the Ministerial authorisation is given.

(4) If a Ministerial authorisation is given orally in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure asset;
the Minister must:
(c) do both of the following:
(i) make a written record of the Ministerial authorisation;
(ii) give a copy of the written record of the Ministerial authorisation to the responsible entity for the asset; and
(d) do so within 48 hours after the Ministerial authorisation is given.

(5) If a Ministerial authorisation is given orally in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure sector asset (other than a critical infrastructure asset);
the Minister must:
(c) make a written record of the Ministerial authorisation; and
(d) give a copy of the written record of the Ministerial authorisation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:

(i) the owner, or each of the owners, of the asset;
(ii) the operator, or each of the operators, of the asset; and

(e) do so within 48 hours after the Ministerial authorisation is given.

*Notification of Ministerial authorisations given in writing*

(6) If a Ministerial authorisation is given in writing in relation to:
(a) a cyber security incident; and
(b) an asset;
the Minister must:
(c) give a copy of the Ministerial authorisation to the Secretary and the Inspector-General of Intelligence and Security; and
(d) do so within 48 hours after the Ministerial authorisation is given.

(7) If a Ministerial authorisation is given in writing in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure asset;
the Minister must:
(c) give a copy of the Ministerial authorisation to the responsible entity for the asset; and
(d) do so within 48 hours after the Ministerial authorisation is given.

(8) If a Ministerial authorisation is given in writing in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure sector asset (other than a critical infrastructure asset);
the Minister must:
(c) give a copy of the Ministerial authorisation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:
(i) the owner, or each of the owners, of the asset;
(ii) the operator, or each of the operators, of the asset; and
(d) do so within 48 hours after the Ministerial authorisation is given.

## 35AF Form of application for Ministerial authorisation

(1) The Secretary may apply for a Ministerial authorisation either:
  (a) orally; or
  (b) in writing.

(2) The Secretary must not apply orally for a Ministerial authorisation that relates to:
  (a) a cyber security incident; and
  (b) an asset;
unless the delay that would occur if the application were to be made in writing would frustrate the effectiveness of:
  (c) any directions that may be given under section 35AK or 35AQ in relation to the incident and the asset; or
  (d) any requests that may be given under section 35AX in relation to the incident and the asset.

(3) If an application for a Ministerial authorisation is made orally, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the application;
    (ii) give a copy of the written record of the application to the Minister; and
  (b) do so within 48 hours after the application is made.

## 35AG Duration of Ministerial authorisation

*Scope*

(1) This section applies if a Ministerial authorisation is given in relation to:
  (a) a cyber security incident; and
  (b) an asset.

*Duration of Ministerial authorisation*

(2) Subject to this section, the Ministerial authorisation remains in force for the period specified in the Ministerial authorisation (which must not exceed 20 days).

*Fresh Ministerial authorisation*

(3) If a Ministerial authorisation (the ***original Ministerial authorisation***) is in force, this Act does not prevent the Minister from giving a fresh Ministerial authorisation that:
  (a) is in the same, or substantially the same, terms as the original Ministerial authorisation; and
  (b) comes into force immediately after the expiry of the original Ministerial authorisation.

(4) In deciding whether to give such a fresh Ministerial authorisation, the Minister must have regard to the number of occasions on which Ministerial authorisations have been made in relation to the incident and the asset.

(5) Subsection (4) does not limit the matters to which the Minister may have regard to in deciding whether to give a fresh Ministerial authorisation.

## 35AH Revocation of Ministerial authorisation

*Scope*

(1) This section applies if a Ministerial authorisation is in force in relation to:
  (a) a cyber security incident; and
  (b) an asset.

*Power to revoke Ministerial authorisation*

(2) The Minister may, in writing, revoke the Ministerial authorisation.

*Duty to revoke Ministerial authorisation*

(3) If the Minister is satisfied that the Ministerial authorisation is no longer required to respond to the incident, the Minister must, in writing, revoke the Ministerial authorisation.

(4) If the Secretary is satisfied that the Ministerial authorisation is no longer required to respond to the incident, the Secretary must:
  (a) notify the Minister that the Secretary is so satisfied; and

(b) do so soon as practicable after the Secretary becomes so satisfied.

*Notification of revocation*

(5) If the Ministerial authorisation is revoked, the Minister must:
(a) give a copy of the revocation to:
(i) the Secretary; and
(ii) the Inspector-General of Intelligence and Security; and
(iii) each relevant entity for the asset; and
(b) do so within 48 hours after the Ministerial authorisation is revoked.

(6) If a Ministerial authorisation is revoked in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure asset;
the Minister must:
(c) give a copy of the revocation to the responsible entity for the asset; and
(d) do so within 48 hours after the Ministerial authorisation is revoked.

(7) If a Ministerial authorisation is revoked in relation to:
(a) a cyber security incident; and
(b) a critical infrastructure sector asset (other than a critical infrastructure asset);
the Minister must:
(c) give a copy of the revocation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:
(i) the owner, or each of the owners, of the asset;
(ii) the operator, or each of the operators, of the asset; and
(d) do so within 48 hours after the Ministerial authorisation is revoked.

*Revocation is not a legislative instrument*

(8) A revocation of the Ministerial authorisation is not a legislative instrument.

*Application of Acts Interpretation Act 1901*

(9) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

### 35AJ Minister to exercise powers personally

A power of the Minister under this Division may only be exercised by the Minister personally.

## Division 3—Information gathering directions

### 35AK Information gathering direction

*Scope*

(1) This section applies if a Ministerial authorisation given under paragraph 35AB(2)(a) or (b) is in force in relation to:
  (a) a cyber security incident; and
  (b) an asset.

*Direction*

(2) If:
  (a) an entity is a relevant entity for the asset; and
  (b) the Secretary has reason to believe that the entity has information that may assist with determining whether a power under this Act should be exercised in relation to the incident and the asset;

the Secretary may direct the entity to:
  (c) give any such information to the Secretary; and
  (d) do so within the period, and in the manner, specified in the direction.

(3) The period specified in the direction must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) The Secretary must not give the direction unless the Secretary is satisfied that:

(a) the direction is a proportionate means of obtaining the information; and

(b) compliance with the direction is technically feasible.

(5) The Secretary must not give a direction that would require an entity to:

(a) do an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or

(b) do an act or thing that would be prohibited by section 108 of the *Telecommunications (Interception and Access) Act 1979*; or

(c) do an act or thing that would (disregarding this Act) be prohibited by section 276, 277 or 278 of the *Telecommunications Act 1997*.

(6) Before giving a direction under this section to an entity, the Secretary must consult the entity unless the delay that would occur if the entity were consulted would frustrate the effectiveness of the direction.

*Other powers not limited*

(7) This section does not, by implication, limit a power conferred by another provision of this Act.

## 35AL Form of direction

(1) A direction under section 35AK may be given:

(a) orally; or

(b) in writing.

(2) The Secretary must not give a direction under section 35AK orally unless the delay that would occur if the direction were to be given in writing would frustrate the effectiveness of the direction.

(3) If a direction under section 35AK is given orally to an entity, the Secretary must:

(a) do both of the following:

(i) make a written record of the direction;

(ii) give a copy of the written record of the direction to the entity; and

(b) do so within 48 hours after the direction is given.

### 35AM Compliance with an information gathering direction

An entity must comply with a direction given to the entity under section 35AK to the extent that the entity is capable of doing so.

Civil penalty: 150 penalty units.

### 35AN Self-incrimination etc.

(1) An entity is not excused from giving information under section 35AK on the ground that the information might tend to incriminate the entity.

(2) If, at general law, an individual would otherwise be able to claim the privilege against self-exposure to a penalty (other than a penalty for an offence) in relation to giving information under section 35AK, the individual is not excused from giving information under that section on that ground.

Note: A body corporate is not entitled to claim the privilege against self-exposure to a penalty.

### 35AP Admissibility of information etc.

If information is given under section 35AK:

(a) the information; or

(b) giving the information;

is not admissible in evidence against an entity:

(c) 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

(d) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of section 35AM.

## Division 4—Action directions

### 35AQ Action direction

(1) If an entity is a relevant entity for:

(a) a critical infrastructure asset; or
(b) a critical infrastructure sector asset;

the Secretary may give the entity a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

(2) The Secretary must not give a direction under this section unless the direction:
(a) is identical to a direction specified in a Ministerial authorisation; and
(b) includes a statement to the effect that the direction is authorised by the Ministerial authorisation; and
(c) specifies the date on which the Ministerial authorisation was given.

Note: A Ministerial authorisation must not be given unless the Minister is satisfied that the direction is reasonably necessary for the purposes of responding to a cyber security incident—see section 35AB.

(3) The period specified in the direction must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) A direction under this section is subject to such conditions (if any) as are specified in the direction.

(5) The Secretary must not give a direction under this section that would require an entity to give information to the Secretary.

*Other powers not limited*

(6) This section does not, by implication, limit a power conferred by another provision of this Act.

## 35AR Form of direction

(1) A direction under section 35AQ may be given:
(a) orally; or
(b) in writing.

(2) The Secretary must not give a direction under section 35AQ orally unless the delay that would occur if the direction were to be given in writing would frustrate the effectiveness of the direction.

(3) If a direction under section 35AQ is given orally to an entity, the Secretary must:

(a) do both of the following:

(i) make a written record of the direction;

(ii) give a copy of the written record of the direction to the entity; and

(b) do so within 48 hours after the direction is given.

## 35AS Revocation of direction

*Scope*

(1) This section applies if:

(a) a direction is in force under section 35AQ in relation to a Ministerial authorisation; and

(b) the direction was given to a particular entity.

*Power to revoke direction*

(2) The Secretary may, by written notice given to the entity, revoke the direction.

*Duty to revoke direction*

(3) If the Secretary is satisfied that the direction is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the entity, revoke the direction.

*Automatic revocation of direction*

(4) If the Ministerial authorisation ceases to be in force, the direction is revoked.

*Application of Acts Interpretation Act 1901*

(5) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

### 35AT Compliance with direction

(1) An entity commits an offence if:
  (a) the entity is given a direction under section 35AQ; and
  (b) the entity engages in conduct; and
  (c) the entity's conduct breaches the direction.

  Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) Subsection (1) does not apply if the entity took all reasonable steps to comply with the direction.

### 35AV Directions prevail over inconsistent obligations

If an obligation under this Act is applicable to an entity, the obligation has no effect to the extent to which it is inconsistent with a direction given to the entity under section 35AQ.

### 35AW Liability

(1) 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 given under section 35AQ.

(2) 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 (1).

## Division 5—Intervention requests

### 35AX Intervention request

(1) The Secretary may give the chief executive of the authorised agency a request that the authorised agency do one or more specified acts or things within the period specified in the request.

(2) The Secretary must not give a request under this section unless the request:
  (a) is identical to a request specified in a Ministerial authorisation; and

(b) includes a statement to the effect that the request is authorised by the Ministerial authorisation; and

(c) specifies the date on which the Ministerial authorisation was given.

Note: A Ministerial authorisation must not be given unless the Minister is satisfied that the request is reasonably necessary for the purposes of responding to a cyber security incident—see section 35AB.

(3) The period specified in the request must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) A request under this section is subject to such conditions (if any) as are specified in the request.

(5) A request under this section does not extend to:

(a) doing an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or

(b) doing an act or thing that would be prohibited by section 108 of the *Telecommunications (Interception and Access) Act 1979*; or

(c) doing an act or thing that would (disregarding this Act) be prohibited by section 276, 277 or 278 of the *Telecommunications Act 1997*.

*Other powers not limited*

(6) This section does not, by implication, limit a power conferred by another provision of this Act.

### 35AY Form and notification of request

(1) A request under section 35AX may be given:

(a) orally; or

(b) in writing.

(2) The Secretary must not give a request under section 35AX orally unless the delay that would occur if the request were to be given in writing would frustrate the effectiveness of the request.

*Notification of requests given orally*

(3) If a request under section 35AX is given orally, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is given.

(4) If a request under section 35AX is given orally in relation to a critical infrastructure asset, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the responsible entity for the asset; and
  (b) do so within 48 hours after the request is given.

(5) If a request under section 35AX is given orally in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:
  (a) make a written record of the request; and
  (b) give a copy of the written record of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:
    (i) the owner, or each of the owners, of the asset;
    (ii) the operator, or each of the operators, of the asset; and
  (c) do so within 48 hours after the request is given.

*Notification of requests given in writing*

(6) If a request under section 35AX is given in writing, the Secretary must:
  (a) give a copy of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is made.

(7) If a request under section 35AX is given in writing in relation to a critical infrastructure asset, the Secretary must:
  (a) give a copy of the request to the responsible entity for the asset; and

(b) do so within 48 hours after the request is given.

(8) If a request under section 35AX is given in writing in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:

(a) give a copy of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:

(i) the owner, or each of the owners, of the asset;

(ii) the operator, or each of the operators, of the asset; and

(b) do so within 48 hours after the request is given.

## 35AZ Compliance with request

(1) The authorised agency is authorised to do an act or thing in compliance with a request under section 35AX.

(2) An act or thing done by the authorised agency in compliance with a request under section 35AX is taken to be done in the performance of the function conferred on the authorised agency by paragraph 7(1)(f) of the *Intelligence Services Act 2001*.

## 35BA Revocation of request

*Scope*

(1) This section applies if a request is in force under section 35AX in relation to a Ministerial authorisation.

*Power to revoke request*

(2) The Secretary may, by written notice given to the chief executive of the authorised agency, revoke the request.

*Duty to revoke request*

(3) If the Secretary is satisfied that the request is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the chief executive of the authorised agency, revoke the request.

*Automatic revocation of request*

(4) If the Ministerial authorisation ceases to be in force, the request is revoked.

*Notification of revocation of request*

(5) If a request under section 35AX is revoked, the Secretary must:
  (a) give a copy of the revocation of the request to the chief executive of the authorised agency and each relevant entity for the asset; and
  (b) do so as soon as practicable after the revocation.

*Application of Acts Interpretation Act 1901*

(6) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

## 35BB Relevant entity to assist the authorised agency

(1) If:
  (a) a request is in force under section 35AX in relation to a critical infrastructure asset or a critical infrastructure sector asset; and
  (b) an entity is a relevant entity for the asset;

an approved staff member of the authorised agency may require the entity to:
  (c) provide the approved staff member with access to premises for the purposes of the authorised agency complying with the request; or
  (d) provide the authorised agency with specified information or assistance that is reasonably necessary to allow the authorised agency to comply with the request.

Note: See also section 149.1 of the *Criminal Code* (which deals with obstructing and hindering Commonwealth public officials).

(2) Paragraph (1)(c) does not apply to premises that are used solely or primarily as a residence.

(3) An entity must comply with a requirement under subsection (1).

Civil penalty: 150 penalty units.

*Liability*

(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 compliance with a requirement under subsection (1).

(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).

## 35BC Constable may assist the authorised agency

(1) If an entity refuses or fails to provide an approved staff member of the authorised agency with access to premises when required to do so under subsection 35BB(1):

(a) the approved staff member may enter the premises for the purposes of the authorised agency complying with the request mentioned in that subsection; and

(b) a constable may:

(i) assist the approved staff member in gaining access to the premises by using reasonable force against property; and

(ii) if necessary for the purposes of so assisting the approved staff member—enter the premises.

(2) If an approved staff member of the authorised agency has entered premises for the purposes of the authorised agency complying with a request under section 35AX, a constable may:

(a) assist the authorised agency in complying with the request by using reasonable force against property located on the premises; and

(b) for the purposes of so assisting the authorised agency—enter the premises.

## 35BD Removal and return of computers etc.

*Removal of computers etc.*

(1) If:

(a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and

(b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the addition or connection of the computer or device is no longer required for the purposes of responding to the cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the approved staff member forms that belief.

(2) If:

(a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and

(b) the request ceases to be in force;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the request ceases to be in force.

*Return of computers etc.*

(3) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the removal of the computer or device is no longer required for the purposes of responding to the cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must return the computer or device as soon as practicable after the approved staff member forms that belief.

(4) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) the request ceases to be in force;

the authorised agency must return the computer or device as soon as practicable after the request ceases to be in force.

### 35BE Use of force against an individual not authorised

This Division does not authorise the use of force against an individual.

### 35BF Liability

Each of the following:

(a) the chief executive of the authorised agency;

(b) an approved staff member of the authorised agency;

(c) a constable;

is not liable to an action or other proceeding (whether civil or criminal) for, or in relation to, an act or matter done or omitted to be done in the exercise of any power or authority conferred by this Division.

### 35BG Evidentiary certificates

(1) The Inspector-General of Intelligence and Security may issue a written certificate setting out any facts relevant to the question of whether anything done, or omitted to be done, by the authorised agency, or an approved staff member of the authorised agency, was done, or omitted to be done, in the exercise of any power or authority conferred by this Division.

(2) A certificate issued under subsection (1) is admissible in evidence in any proceedings as prima facie evidence of the matters stated in the certificate.

### 35BH Chief executive of the authorised agency to report to the Defence Minister and the Minister

(1) If:

(a) the Secretary gives a request under section 35AX that was authorised by a Ministerial authorisation; and

(b) the authorised agency does one or more acts or things in compliance with the request;

the chief executive of the authorised agency must:

(c) prepare a written report that:

(i) sets out details of those acts or things; and

(ii) explains the extent to which doing those acts or things has amounted to an effective response to the cyber security incident to which the Ministerial authorisation relates; and

(d) give a copy of the report to the Defence Minister; and

(e) give a copy of the report to the Minister.

(2) The chief executive of the authorised agency must comply with subsection (1) as soon as practicable after the end of the period specified in the request and, in any event, within 3 months after the end of the period specified in the request.

### 35BJ Approved staff members of the authorised agency

(1) The chief executive of the authorised agency may, in writing, declare that a specified staff member of the authorised agency is an ***approved staff member of the authorised agency*** for the purposes of this Act.

(2) A declaration under subsection (1) is not a legislative instrument.

## Division 6—Reports to the Parliamentary Joint Committee on Intelligence and Security

### 35BK Reports to the Parliamentary Joint Committee on Intelligence and Security

(1) If the Secretary gives one or more directions under section 35AK or 35AQ, or one or more requests under section 35AX, in relation to a cyber security incident, the Secretary must give the Parliamentary Joint Committee on Intelligence and Security a written report about the incident.

(2) The report must include a description of each of the directions or requests.

## 46 Section 36 (paragraph beginning "Information")

Repeal the paragraph.

## 47 At the end of section 36

Add:

Note: Protected information is defined in section 5.

## 48 Subparagraph 42(2)(a)(viii)

Omit "industry for the critical infrastructure asset", substitute "critical infrastructure sector".

## 49 Paragraph 42(2)(b)

Omit "industry for the critical infrastructure asset", substitute "critical infrastructure sector".

## 50 After section 43

Insert:

### 43A Authorised disclosure to IGIS official

The Secretary may:

(a) disclose protected information to an IGIS official for the purposes of exercising powers, or performing duties or functions, as an IGIS official; and

(b) make a record of or use protected information for the purpose of that disclosure.

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

### 43B Authorised use and disclosure—Ombudsman official

Protected information may be disclosed by an Ombudsman official to an IGIS official for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

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

### 43C Authorised use and disclosure—IGIS official

Protected information may be disclosed by an IGIS official to an Ombudsman official for the purposes of the Ombudsman official exercising powers, or performing functions or duties, as an Ombudsman official.

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

### 43D Authorised use and disclosure—ASD

The Director-General of ASD or a staff member of ASD may make a record of, use or disclose protected information for the purposes of the performance of the functions of ASD set out in section 7 of the *Intelligence Services Act 2001*.

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

## 51 Paragraph 45(1)(a)

Repeal the paragraph, substitute:

(a) the entity:

(i) obtains information; or

(ii) generates information for the purposes of complying with this Act; and

## 52 Paragraph 45(1)(d)

Omit "subsection 51(3) or 52(4)", substitute "a notification provision".

## 53 Paragraph 46(1)(a)

Omit "subsection 51(3) or 52(4)", substitute "a notification provision".

## 54 Subsection 46(3)

Omit "subsection 51(3) or 52(4)", substitute "a notification provision".

## 54A Section 47

Omit "Except where it is necessary to do so for the purposes of giving effect to this Act, an entity is not", substitute "(1) An entity is not (subject to subsection (2))".

## 54B At the end of section 47

Add:

(2) Subsection (1) does not prevent an entity from being required to disclose protected information, or to produce a document containing protected information, if it is necessary to do so for the purposes of giving effect to:

(a) this Act; or

(b) the *Inspector-General of Intelligence and Security Act 1986*, or any other Act that confers functions, powers or duties on the Inspector-General of Intelligence and Security; or

(c) a legislative instrument made under an Act mentioned in paragraph (a) or (b).

## 55 At the end of section 48

Add:

> Infringement notices may be given under Part 5 of the Regulatory Powers Act for alleged contraventions of certain provisions of this Act.
>
> A provision is subject to monitoring under Part 2 of the Regulatory Powers Act if it is:
>
> (a) an offence against section 35AT or 45 of this Act; or
>
> (b) a civil penalty provision of this Act.
>
> A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is:
>
> (a) an offence against section 35AT or 45 of this Act; or
>
> (b) a civil penalty provision of this Act.

## 56 Subsections 49(2) and (3)

Repeal the subsections, substitute:

*Authorised applicant*

(2) For the purposes of Part 4 of the Regulatory Powers Act, as that Part applies in relation to a civil penalty provision of this Act, each of the following persons is an authorised applicant:

(a) the Secretary;
(b) a person who is appointed under subsection (3).

(3) The Secretary may, by writing, appoint a person who:
(a) is the chief executive officer (however described) of a relevant Commonwealth regulator; or
(b) is an SES employee, or an acting SES employee, in:
(i) the Department; or
(ii) a relevant Commonwealth regulator; or
(c) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant for the purposes of Part 4 of the Regulatory Powers Act, as that Part applies in relation to a civil penalty provision of this Act.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

*Authorised person*

(3A) For the purposes of Parts 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act, each of the following persons is an authorised applicant:
(a) the Secretary;
(b) a person who is appointed under subsection (3B).

(3B) The Secretary may, by writing, appoint a person who:
(a) is the chief executive officer (however described) of a relevant Commonwealth regulator; or
(b) is an SES employee, or an acting SES employee, in:
(i) the Department; or
(ii) a relevant Commonwealth regulator; or
(c) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant for the purposes of Parts 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

## 57 At the end of Part 5

Add:

# Division 3—Monitoring and investigation powers

### 49A Monitoring powers

*Provisions subject to monitoring*

(1) A provision is subject to monitoring under Part 2 of the Regulatory Powers Act if it is:

(a) an offence against section 35AT or 45; or

(b) a civil penalty provision of this Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the provisions have been complied with. It includes powers of entry and inspection.

*Information subject to monitoring*

(2) Information given in compliance or purported compliance with a provision of this Act is subject to monitoring under Part 2 of the Regulatory Powers Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of entry and inspection.

*Authorised applicant*

(3) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (4) is an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(4) The Secretary may, by writing, appoint a person who:

(a) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a relevant Commonwealth regulator; or

(b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

*Authorised person*

(5) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (6) is an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(6) The Secretary may, by writing, appoint a person who is:

(a) an APS employee in:

(i) the Department; or

(ii) a relevant Commonwealth regulator; or

(b) an officer or employee of a relevant Commonwealth regulator;

to be an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

*Issuing officer*

(7) For the purposes of Part 2 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

*Relevant chief executive*

(8) For the purposes of Part 2 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(9) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (10) to a person who is an SES employee, or an acting SES employee, in the Department.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

(10) The powers and functions that may be delegated are:

(a) powers under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2); and

(b) powers and functions under the Regulatory Powers Act that are incidental to a power mentioned in paragraph (a).

(11) A person exercising powers or performing functions under a delegation under subsection (9) must comply with any directions of the relevant chief executive.

*Relevant court*

(12) For the purposes of Part 2 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2):

(a) the Federal Court of Australia;

(b) the Federal Circuit Court of Australia; and

(c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

*Premises*

(13) An authorised person must not enter premises under Part 2 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2), if the premises are used solely or primarily as a residence.

*Person assisting*

(14) An authorised person may be assisted by other persons in exercising powers, or performing functions or duties, under Part 2 of the Regulatory Powers Act in relation to the provisions

mentioned in subsection (1) and information mentioned in subsection (2).

*External Territories*

(15) Part 2 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2), extends to every external Territory.

## 49B Investigation powers

*Provisions subject to investigation*

(1) A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is:
  (a) an offence against section 35AT or 45; or
  (b) a civil penalty provision of this Act.

*Authorised applicant*

(2) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (3) is an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).

(3) The Secretary may, by writing, appoint a person who:
  (a) is an SES employee, or an acting SES employee, in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

*Authorised person*

(4) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (5) is an authorised person in

relation to evidential material that relates to a provision mentioned in subsection (1).

(5) The Secretary may, by writing, appoint a person who is:

(a) an APS employee in:

(i) the Department; or

(ii) a relevant Commonwealth regulator; or

(b) an officer or employee of a relevant Commonwealth regulator;

to be an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1).

*Issuing officer*

(6) For the purposes of Part 3 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to evidential material that relates to a provision mentioned in subsection (1).

*Relevant chief executive*

(7) For the purposes of Part 3 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to evidential material that relates to a provision mentioned in subsection (1).

(8) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (9) to a person who is an SES employee or an acting SES employee in the Department.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

(9) The powers and functions that may be delegated are:

(a) powers under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1); and

(b) powers and functions under the Regulatory Powers Act that are incidental to a power mentioned in paragraph (a).

(10) A person exercising powers or performing functions under a delegation under subsection (8) must comply with any directions of the relevant chief executive.

*Relevant court*

(11) For the purposes of Part 3 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to evidential material that relates to a provision mentioned in subsection (1):

(a) the Federal Court of Australia;

(b) the Federal Circuit Court of Australia;

(c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

*Person assisting*

(12) An authorised person may be assisted by other persons in exercising powers, or performing functions or duties, under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1).

*External Territories*

(13) Part 3 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1), extends to every external Territory.

## Division 4—Infringement notices

### 49C Infringement notices

*Provisions subject to an infringement notice*

(1) A civil penalty provision of this Act is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

*Infringement officer*

(2) For the purposes of Part 5 of the Regulatory Powers Act, a person authorised under subsection (3) is an infringement officer in relation to the provisions mentioned in subsection (1).

(3) The Secretary may, by writing, authorise a person who:

(a) is an SES employee, or an acting SES employee, in:
(i) the Department; or
(ii) a relevant Commonwealth regulator; or
(b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an infringement officer in relation to the provisions mentioned in subsection (1).

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

*Relevant chief executive*

(4) For the purposes of Part 5 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the provisions mentioned in subsection (1).

(5) The relevant chief executive may, in writing, delegate any or all of the relevant chief executive's powers and functions under Part 5 of the Regulatory Powers Act to a person who is an SES employee or an acting SES employee in the Department.

Note: The expressions ***SES employee*** and ***acting SES employee*** are defined in section 2B of the *Acts Interpretation Act 1901*.

(6) A person exercising powers or performing functions under a delegation under subsection (5) must comply with any directions of the relevant chief executive.

*External Territories*

(7) Part 5 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1), extends to every external Territory.

## 58 Paragraphs 51(1)(b) and (c)

Repeal the paragraphs, substitute:

(b) the asset relates to a critical infrastructure sector; and
(c) the Minister is satisfied that the asset is critical to:
(i) the social or economic stability of Australia or its people; or

(ii) the defence of Australia; or
(iii) national security; and

(d) there would be a risk to:
(i) the social or economic stability of Australia or its people; or
(ii) the defence of Australia; or
(iii) national security;
if it were publically known that the asset is a critical infrastructure asset.

## 59 Subsection 51(1) (note 1)

Repeal the note.

## 60 Subsection 51(1) (note 2)

Omit "Note 2", substitute "Note".

## 61 After subsection 51(2)

Insert:

(2A) The declaration may do any or all of the following:
(a) determine that Part 2 applies to the asset;
(c) determine that Part 2B applies to the asset.

## 62 Paragraph 51(3)(b)

Repeal the paragraph, substitute:

(b) if the asset is a tangible asset located (wholly or partly) in a State, the Australian Capital Territory or the Northern Territory—the First Minister of the State, the Australian Capital Territory or the Northern Territory, as the case requires.

## 63 Subsection 51(4)

Repeal the subsection.

## 64 After section 51

Insert:

### 51A Consultation—declaration

(1) Before making a declaration under section 51 that specifies an entity as the responsible entity for an asset, the Minister must give the entity a notice:
  (a) setting out the proposed declaration; and
  (b) inviting the entity to make submissions to the Minister about the proposed declaration within:
    (i) 28 days after the notice is given; or
    (ii) if a shorter period is specified in the notice—that shorter period.

(2) The Minister must consider any submissions received within:
  (a) the 28-day period mentioned in subparagraph (1)(b)(i); or
  (b) if a shorter period is specified in the notice—that shorter period.

(3) The Minister must not specify a shorter period in the notice unless the Minister is satisfied that the shorter period is necessary due to urgent circumstances.

(4) The notice must set out the reasons for making the declaration, unless the Minister is satisfied that doing so would be prejudicial to security.

## 65 Subsection 52(5)

Repeal the subsection.

## 67 Subsection 59(1)

After "this Act", insert "(other than Part 3A)".

## 68 Division 4 of Part 7 (at the end of the heading)

Add "**etc.**".

## 69 At the end of subsection 60(2)

Add:

; and (h) the number of cyber security incidents reported during the financial year under section 30BC; and

(i) the number of cyber security incidents reported during the financial year under 30BD; and

(n) the number of Ministerial authorisations given under section 35AB during the financial year; and

(o) the number of Ministerial authorisations given under paragraph 35AB(2)(a) or (b) during the financial year; and

(p) the number of Ministerial authorisations given under paragraph 35AB(2)(c) or (d) during the financial year; and

(q) the number of Ministerial authorisations given under paragraph 35AB(2)(e) or (f) during the financial year.

## 70 After section 60

Insert:

### 60AA Compensation for acquisition of property

(1) If the operation of this Act would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from an entity otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the entity.

(2) If the Commonwealth and the entity do not agree on the amount of the compensation, the entity may institute proceedings in:

(a) the Federal Court of Australia; or

(b) the Supreme Court of a State or Territory;

for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

### 60AB Service of notices, directions and instruments by electronic means

Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* do not apply to a notice, direction or instrument under:

(a) this Act; or

(b) the rules; or

(c) the Regulatory Powers Act, so far as that Act relates to this Act.

Note: Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* deal with the consent of the recipient of information to the information being given by way of electronic communication.

## 70A After section 60A

Insert:

### 60B Review of this Act

The Parliamentary Joint Committee on Intelligence and Security may:

(a) review the operation, effectiveness and implications of this Act; and

(b) report the Committee's comments and recommendations to each House of the Parliament;

so long as the Committee begins the review before the end of 3 years after the *Security Legislation Amendment (Critical Infrastructure) Act 2021* receives the Royal Assent.

# Part 2—Application provisions

## 71 Application—subsections 9(3) and (4) of the *Security of Critical Infrastructure Act 2018*

The amendments of subsections 9(3) and (4) of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to rules made after the commencement of this item.

## 72 Application—section 51 of the *Security of Critical Infrastructure Act 2018*

The amendments of section 51 of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to a declaration made after the commencement of this item.

# Part 3—Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2021

## *Security of Critical Infrastructure Act 2018*

### 73 Paragraphs 49A(12)(b) and 49B(11)(b)

Omit "Federal Circuit Court of Australia", substitute "Federal Circuit and Family Court of Australia (Division 2)".

# Part 4—Amendments contingent on the commencement of the National Emergency Declaration Act 2020

## *National Emergency Declaration Act 2020*

### 74 Section 10 (after paragraph (za) of the definition of *national emergency law*)

Insert:

(zaa) section 35AB of the *Security of Critical Infrastructure Act 2018*;

## *Security of Critical Infrastructure Act 2018*

### 75 After subsection 35AB(1)

Insert:

(1A) This section also applies if the Minister is satisfied that:

(a) a cyber security incident:

(i) has occurred; or

(ii) is occurring; or

(iii) is imminent; and

(b) the incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset (the ***primary asset***); and

(c) the incident relates to an emergency specified in a national emergency declaration (within the meaning of the *National Emergency Declaration Act 2020*) that is in force; and

(d) no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

# Schedule 2—Australian Signals Directorate

## *Criminal Code Act 1995*

### 1 Subsection 476.4(2) of the *Criminal Code*

Omit "section 476.5", substitute "sections 476.5 and 476.6".

### 2 Section 476.5 of the *Criminal Code* (at the end of the heading)

Add "**—ASIS and AGO**".

### 3 Subsection 476.5(1) of the *Criminal Code*

Omit "ASIS, AGO or ASD", substitute "ASIS or AGO".

### 4 Subsection 476.5(3) of the *Criminal Code* (definition of *ASD*)

Repeal the definition.

### 5 Subsection 476.5(3) of the *Criminal Code* (paragraph (b) of the definition of *staff member*)

Repeal the paragraph.

### 6 At the end of Division 476 of the *Criminal Code*

Add:

#### 476.6 Liability for certain acts—ASD

(1) A staff member or agent of ASD is not subject to any civil or criminal liability for engaging in conduct inside or outside Australia if:

(a) the conduct is engaged in on the reasonable belief that it is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia); and

(b) the conduct is engaged in in the proper performance of a function of ASD.

(2) A person is not subject to any civil or criminal liability for engaging in conduct inside or outside Australia if:

(a) the conduct is preparatory to, in support of, or otherwise directly connected with, overseas activities of ASD; and

(b) the conduct:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the conduct is engaged in in the proper performance of a function of ASD.

(3) Subsection (2) is not intended to permit any conduct in relation to premises, persons, computers, things, or carriage services in Australia, being:

(a) conduct which ASIO could not engage in without a Minister authorising it by warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*; or

(b) conduct engaged in to obtain information that ASIO could not obtain other than in accordance with Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*.

(4) Subsections (1) and (2) have effect despite anything in a law of the Commonwealth or of a State or Territory, whether passed or made before or after the commencement of this subsection, unless the law expressly provides otherwise.

(5) Subsection (4) does not affect the operation of subsection (3).

*Certificate*

(6) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether conduct was engaged in in the proper performance of a function of ASD.

(7) In any proceedings, a certificate given under subsection (6) is prima facie evidence of the facts certified.

*Notice to Inspector-General of Intelligence and Security*

(8) If:

(a) a person engages in conduct referred to in subsection (1) or (2) in relation to ASD; and

(b) the conduct causes material damage, material interference or material obstruction to a computer (within the meaning of section 22 of the *Australian Security Intelligence Organisation Act 1979*) in Australia; and

(c) apart from this section, the person would commit an offence against this Part;

then the agency head (within the meaning of the *Intelligence Services Act 2001*) of ASD must, as soon as practicable, give a written notice to the Inspector-General of Intelligence and Security that:

(d) informs the Inspector-General of Intelligence and Security of that fact; and

(e) provides details about the conduct that caused the damage, interference or obstruction to the computer.

(9) This section has effect in addition to, and does not limit, section 14 of the *Intelligence Services Act 2001*.

*Definitions*

(10) In this section:

***ASD*** means the Australian Signals Directorate.

***civil or criminal liability*** means any civil or criminal liability (whether under this Part, under another law or otherwise).

***computer-related act, event, circumstance or result*** means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device; or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.

***staff member***, in relation to ASD, means:

(a) the Director-General of ASD; or

(b) a member of the staff of ASD (whether an employee of ASD, a consultant or contractor to ASD, or a person who is made available by another Commonwealth or State authority or other person to perform services for ASD).

## 7 Application of amendments

The amendments made by this Schedule apply in relation to conduct engaged in after the commencement of this Schedule.

[*Minister's second reading speech made in—*
*House of Representatives on 10 December 2020*
*Senate on 21 October 2021*]

(182/20)